RSA NetWitness

Version 11.7

NetWitness UEBA User Guide

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

April 2022

Contents

Introduction

RSA NetWitness User and Entity Behavior Analytics (UEBA) is an advanced analytics solution that empowers enterprise SOC managers and analysts to discover, investigate, and monitor risky behaviors across entities namely Users and Network (packets) in your environment.

NetWitness UEBA enables analyst to:

- Detect
  - malicious and rogue users
  - abnormal network traffic
- Identify high-risk behaviors
- Discover attacks
- Investigate emerging security threats
- Identify potential attacker's activity

This guide provides information and instructions for using the NetWitness UEBA functionalities and capabilities. It describes the key investigation methodologies, the main system capabilities, common use cases, and step-by-step instructions for the recommended workflow strategies.

Users

UEBA helps to analyze all users in your organization using logs and endpoint data for user activities, which is retrieved and parsed from the NetWitness Database (NWDB).
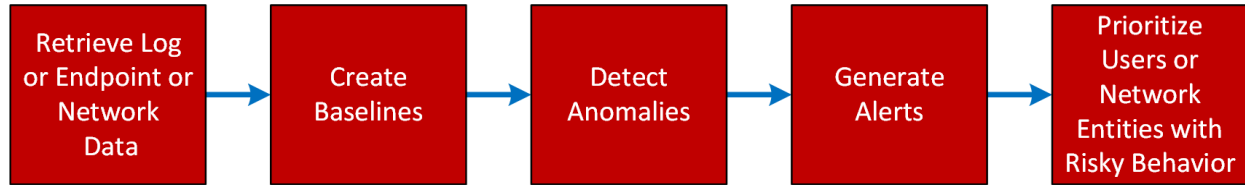
Network

> **Note:** Network entities are supported on RSA NetWitness Platform 11.4 and later.

UEBA helps to analyze malicious outbound traffic masked within a legitimate HTTPS session. It can detect various network abnormalities, such as abnormal outbound traffic volume sent to a specific port, domain, organization or SSL Subject. The network (packet) data is retrieved and parsed from the NWDB into the new TLS data source, which supports two new entities: JA3 and SSL Subject. These entities validate the false negatives and true positives, and detect abnormal network traffic for JA3 and SSL Subject fingerprints.

- **JA3** - JA3 is a method of creating client-side SSL/TLS fingerprints to identify the client application initiating the session. The JA3 fingerprints perform JA3-signature-based analysis and detect abnormal network traffic, such as abnormal number of bytes sent over HTTPS.

- **SSL Subject** - The subject field of the certificate identifies the entity associated with the public key stored in the subject public key field, which is the entity for which the certificate was issued.

How NetWitness UEBA Works

NetWitness UEBA uses analytics to detect anomalies in the log and endpoint or network data to derive behavioral results from them. The following diagram displays the basic workflow:

Retrieve Log or Endpoint or Network Data → Create Baselines → Detect Anomalies → Generate Alerts → Prioritize Users or Network Entities with Risky Behavior

The following table provides a brief description of each step.

Step	Description	More Information
1. Retrieve Log and Endpoint or Network Data	NetWitness UEBA retrieves logs or endpoint or network data from the NWDB and uses the data to create analytic results.	See Retrieve Data
2. Create Baselines	Baselines are derived from detailed analysis of normal user or network entity behavior, and are used as a basis for comparison to user or network entity behavior over time.	See Create Baselines
3. Detect Anomalies	An anomaly is a deviation of a user or network entity from the normal baseline behavior. NetWitness UEBA performs statistical analysis to compare each new activity to the baseline. User or network entity activities that deviate from expected baseline values are scored accordingly to reflect the severity of the deviation.	See Detect Anomalies
4. Generate Alerts	All the anomalies found in step 3 are grouped into hourly batches. Each batch is scored based on the uniqueness of its indicators. If the indicator composition is unique compared to a user or network entity's historic hourly batch compositions, it is likely that this batch is transformed into an alert.	See Generate Indicators and Generate Alerts
5. Prioritize User or Network Entities with Risky Behavior	NetWitness UEBA prioritizes the potential risk from a user or network entity by using a simplified additive scoring formula. Each alert is assigned a severity that increases a user or network entity's score by a predefined number of points. User or network entity with high scores either have multiple alerts, or alerts of high levels of severity associated with them.	See Prioritize User or Network Entity with Risky Behavior

Retrieve Data

NetWitness UEBA connects to a Concentrator service to retrieve log and endpoint data for the user entity or network data for the network entities. In case of multiple Concentrators, the NetWitness UEBA server connects to a Broker service. You can use the Broker service that is available on the NetWitness Platform Admin server if you do not have an exclusive Broker in your deployment. During NetWitness UEBA installation, the administrator specifies the IP address of the Broker service. For more information, see the "(Optional) Task 2 - Install NetWitness UEBA" topic in the *NetWitness Platform 11.5 Physical Host Installation Guide*

Note: In 11.4 and later, and when installed on a virtual machine, UEBA can process up to 20 million network events per day. For more information to resolve these issues, see the 'Troubleshooting UEBA Configurations' topic in the *UEBA Configuration Guide*.

Create Baselines

NetWitness UEBA uses machine learning to analyze multiple aspects of a user or network entity behavior within a stream of log and endpoint or network data and gradually builds a multi-dimensional baseline of typical behavior for each user or network entity.

Behavioral baselines are also created on a global level to describe common activities observed throughout the network. For example, if a working hour is abnormal for a user entity, but is not abnormal for the organization, the false-positive reduction algorithms decrease the impact on the alert score. Models are updated frequently and are constantly improving as time goes on.

Note: NetWitness UEBA requires 28 days of historical log and endpoint data for users and network data for network entities to create a proper baseline for all entities in your network. However, RSA recommends that you configure NetWitness UEBA to start baselining your data two months before the deployment date `<today-60days>`. The first 28 days are used for model training and are not scored. The remaining 32 days are leveraged to improve and update the model, and are also scored to provide initial value.

Note: For version 11.2 or later, there is limited support for environments with multiple domains. Distinct username values that are registered under different domains are normalized, and combined into one modeled entity. As a result, different users, who share the same username in different domains, will incorrectly be attributed to a single normalized entity.

Create Baselines for Users

NetWitness UEBA analyzes user actions to build a multi-dimensional baseline that reflects the typical behavior of the user. For example, the baseline can include information about the hours in which a user typically logs on.

Create Baselines for Network

NetWitness UEBA analyzes the network traffic pattern of JA3 or SSL Subject within a stream of network data to create a multi-dimensional baseline. For example, the baseline can be the allowed limit of data sent from an application or specific port that is connected to an application.

Detect Anomalies

The data is parsed hourly, to detect abnormal behavior. After establishing a behavioral baseline for all entities in your environment, each incoming event is compared to the baseline, to determine abnormalities. Based on the deviation the event is scored. The score is high if the deviation is strong and vice-versa. If anomalies are detected, they are turned into indicators that can be viewed on the user interface (UI).

For example, if a user's normal working hours are 9:00 AM to 5:00 PM, a new activity at 6:00 PM or 7:00 PM is not a strong deviation, and is probably not scored as an anomaly. However, an authentication at midnight is a strong deviation and is scored as an anomaly.

For example, in an organization, when a session is authenticated into a website for a SSL handshake, and communicates to five different ports or domains, it is not a strong deviation, and is probably not scored as an anomaly. But if the website communicates to an abnormal port or domain, it is a strong deviation. This indicates an abnormal behavior and is scored as an anomaly and triggers an alert.

Generate Indicators

If anomalies are detected, they are turned into indicators. NetWitness UEBA uses indicators to define validated anomalous activities. Indicators represent anomalies found in either a single event or multiple events batched over time.

User Indicators

User behavior or abnormal user activities, such as suspicious user logons, brute-force password attacks, unusual user changes, and abnormal file access are anomalous activities. Every anomalous activity is associated to an indicator. For more information, see Indicators for Users

Network Indicators

Network behavior or abnormal network traffic that contribute to data exfiltration or phishing, are examples of anomalous activities. Every anomalous activity is associated to an indicator. For more information, see Indicators for Network Entities.

Generate Alerts

All anomalies that are found are grouped into hourly batches by the user or network entity name. Each batch is scored based on the uniqueness of the composition of its indicators. If a composition is unique compared to the user or network entity's history, it is likely that this batch is transformed into an alert, and the anomalies into indicators. A high-scored batch of anomalies becomes an alert that contains valid indicators of compromise.

An abnormal activity by itself, even if it happens hundreds of times a day in a large corporate environment, does not necessarily reflect an account compromise. However, an abnormal behavior that occurs with a lot of other abnormal behaviors can indicate that the account is compromised and is an indication that additional analysis is required.

For example, if the following combination of one or more abnormal user or network behaviors occur, an alert is triggered.

Users

- Authentication from an abnormal computer.
- Multiple authentication attempts identified in a short time frame.
- Multiple files are deleted by this user from the corporate file share.
- Download or transfer files larger that the allowed limits.

Network

- Abnormal destination port for source netname.
- Abnormal organization for source netname.
- Abnormal traffic volume sent to organization.
- Abnormal traffic volume sent to port.

Note: The NetWitness UEBA User Interface can initially appear as empty because alerts are not generated until the baselines are established. If there is no historical audit data when NetWitness UEBA is enabled, the system starts generating the baselines from the time it is deployed, and requires 28 full days to elapse before generating new alerts. If historical audit data is processed when NetWitness UEBA is enabled, alerts appear after the historical data is processed, usually within two to four days.

Prioritize User or Network Entity with Risky Behavior

The entities scores are a primary tool for incident prioritization. The entities score is based on a simple additive calculation of an entity's alerts. Alerts and analyst feedback are the only factors in the entities score calculation, with the impact on the scores determined by their levels of severity. A unified color code is used for entities and alert scores:

Severity	Color	Score
Critical	Red	+20
High	Orange	+15
Medium	Yellow	+10
Low	Green	+1

Supported Sources

Log Sources

NetWitness UEBA natively supports the following data sources:

- Windows Active Directory in Version 11.2
- Windows Logon and Authentication Activity in Version 11.2
- Windows File Servers in Version 11.2
- Windows Remote Management in Version 11.3.2
- NetWitness Endpoint Process in Version 11.3
- NetWitness Endpoint Registry in Version 11.3
- RSASecurID Token in Version 11.3.1
- RedHat Linux in Version 11.3.1
- VPN Logs in Version 11.5
- Azure Active Directory Logs in Version 11.5

Network Sources

- TLS in Version 11.4

Recommended Workflows

To use NetWitness UEBA more effectively, there are two workflows - Detection and Forensic workflow.

Detection Workflow

The detection workflow gives you an overview of the health of your environment, and then focuses on investigating the top high-risk users, entities, and alerts that are displayed in the Overview tab.

The following flowchart illustrates the steps to follow for detecting suspicious behavior in your environment.

| View top 10 users, or entities, or top 10 alerts | → | Investigate details of users, entities, and alerts | → | Determine the result of the investigation | → | Take action to resolve the issues found |

The following table describes each step in the workflow.

Step	Description	Instructions
View top ten users, or entities, or top 10 alerts,	In the Overview tab, note the users and network entity with the risky behaviors and the top most critical alerts.	Investigate High-Risk User or Network Entity and Investigate Top Alerts
Investigate details of users, entities, and alerts	Drill-down into detailed information about risky user or entity behaviors and critical alerts to determine the cause of these actions and how to resolve them.	Investigate High-Risk User or Network Entity and Investigate Events
Determine the result of the investigation	Analyze the summary information provided in the UI from the previous steps and identify focus areas on to resolve the issues.	Identify High-Risk User or Network Entity and Investigate Events
Take action to resolve the issues found	Target specific user or entity behaviors and events to address, and use results of this investigation to improve and sharpen future investigations.	Take Action on High-Risk User or Network Entity

Forensic Workflow

The forensic workflow is recommended when you have an understanding of the typical user or entity behaviors and anomalies in your environment, and helps you focus on specific forensic information that is based on a user or entity behavior, or a specific time frame in which suspicious events occurred.

Using forensics information, analysts may determine actions and behaviors that the attacker is likely to attempt using the following questions:

- What fundamental techniques and behaviors are common across all intrusions?

- What evidence do these techniques leave behind?

- What do attackers do?

- What are normal behaviors of my accounts and entities?

- Which are my sensitive machines and where are they located?

The following flowchart illustrates how to perform investigation on forensic information that is based on a specific user or entity behavior, or a specific time frame in which suspicious events occurred.

The following table describes each step in the workflow.

Step	Description	Instructions
Gain knowledge of expected behaviors and anomalies in your environment	Establish a baseline of normal behaviors, expected anomalies, and unexpected anomalies, to focus on anomalies that are significant for your environment.	Retrieve Data , Detect Anomalies, and Generate Alerts .
Investigate a user or network entity with top score for a specific behavior	Select a user or network entity with a high score for a specific behavior and gather detailed information.	Investigate High-Risk User or Network Entity and Investigate Events.
Investigate alerts that occur in a specific time frame	Determine a time frame of interest, and in the Alerts tab, select that time frame to see detailed information about alerts that occurred during that period.	Investigate Events

Step	Description	Instructions
Determine the result of the investigation	Based on your knowledge of expected user or network entity behavior, focus on the indicators that are displayed during the specified time period and determine if the anomalies that were discovered need to be resolved.	Investigate Events and Identify High-Risk Entities
Take action to resolve the issues found	Target specific user or network entity behaviors and events to address, and use the results of this investigation to improve and sharpen future investigations.	Take Action on High-Risk User or Network Entity

NetWitness UEBA Use Cases

NetWitness UEBA focuses on providing advanced detection capabilities to guard enterprises from insider threats. These could either be compromised trusted users or network entity within a network, or alternatively, an external attacker malicious taking advantage of credentials acquired by using advanced account takeover techniques.

Identity theft typically begins with the theft of credentials, which are then used to obtain unauthorized access to resources and to gain control over the network. Attackers may also exploit compromised non-admin users to obtain access to resources for which they have administrative rights, and then escalate those privileges.

NetWitness UEBA helps you separate possibly malicious activity from the otherwise abnormal, but not risky, user or network entity actions.

Use Case for Users

An attacker who uses stolen credentials may trigger suspicious network events while accessing resources. Detecting illicit credential use is possible, but requires that you separate attacker activity from the high volume of legitimate events. The following use cases define certain risk types, and the corresponding system capabilities used for their detection. You can review the use cases, represented by their alert type and description, to gain an initial understanding of the related risky behavior of each use case. Using NetWitness UEBA, you can then drill down into the indicators that reflect the possibly risky user activities to learn more. For more information about NetWitness UEBA-supported indicators, see Indicators for Users. When anomalies are detected, they are compared to the baseline and compiled into hourly alerts. For more information on types of alerts for Users, see Alert Types for a User .

Use Case for Network Entities

UEBA can detect malicious traffic masked within a legitimate HTTPS session. Based on this alert analysis, the analyst can drill down to the indicators and determine if the activity was normal or not. For more information about NetWitness UEBA-supported entity indicators, see Indicators for Network Entities. For example, the analyst can detect if there was any abnormal number of bytes sent to a port or a domain. If this type of events or a combination of such events are detected an alert is triggered. For more information on types of alerts for network entity, see Alert Types for Network Entities.

Alert Types

Alert Types for a User

Alert Type	Description
Mass Changes to Groups	An abnormal number of changes are made to groups. Investigate which elements are changed, and decide if the changes were legitimate or possibly the result of risky or malicious behavior. This activity is associated with the **Multiple Group Membership Changes** indicator.
Multiple Failed Logons	In traditional password cracking attempts, the attacker tries to obtain a password through guesswork or by employing other low-tech methods to gain initial access. The attacker risks getting caught or being locked out by explicitly attempting to authenticate; but with some prior knowledge of the victim's password history, may be able to successfully authenticate. Look for additional abnormal indications that the account owner is not the one attempting to access this account. This activity is usually associated with the **Multiple Failed Authentications** indicator.
User Login to Abnormal Host	Attackers often need to reacquire credentials and perform other sensitive activities, like using remote access. Tracing the access chain backwards may lead to the discovery of other computers involved in possibly risky activity. If an attacker's presence is limited to a single compromised host or to many compromised hosts, that activity can be associated with the **Abnormal Host** indicator.
Data Exfiltration	Data exfiltration is the unauthorized copying, transfer, or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various techniques, typically by cyber criminals over the Internet or other network. This activity can be associated with the **Excessive Number of File Rename Events**, **Excessive Number of Files Moved from File System**, and **Excessive Number of Files Moved to File System** indicators.
Mass File Rename	Ransomware is a type of malware that encrypts desktop and system files, making them inaccessible. Some ransom ware, for example, Locky, encrypts and renames files as part of their initial execution. Use this indication of mass-file-renaming to determine if your file system is infected with ransomware. This activity can be associated with the **Multiple File Rename Events** indicator.

Alert Type	Description
Snooping User	Snooping is unauthorized access to another person's or company's data. Snooping can be as simple as the casual observance of an e-mail on others computer, or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device. This activity can be associated with the **Multiple File Access Events**, **Multiple Failed File Access Events**, **Multiple File Open Events**, and **Multiple Folder Open Events** indicators.
Multiple Logons by User	All authentication activity, malicious or not, appears as normal logons. Therefore, administrators should monitor unexpected authorized activity. The key is that attackers use these stolen credentials for unauthorized access, which may provide an opportunity for detection. When an account is used for unusual activities, for example, authenticating an unusual amount of times, the account may have been compromised. This activity can be associated with the **Multiple Successful Authentications** indicator.
User Logged into Multiple Hosts	Attackers typically need to reacquire credentials periodically. This is because their key chain of stolen credentials naturally degrades over time, due to password changes and resets. Therefore, attackers frequently maintain a foothold in the compromised organization by installing backdoors and maintaining credentials from many computers in the environment. This activity can be associated with the **Logged onto Multiple Hosts** indicator.
Mass Permission Changes	Some credential theft techniques, for example, Pass-the-Hash, use an iterative, two-stage process. First, an attacker obtains elevated read-write permission to privileged areas of volatile memory and file systems, which are typically accessible only to system-level processes on at least one computer. Second, the attacker attempts to increase access to other computers on the network. Investigate if abnormal permission changes have taken place on the file systems to ensure that they were not compromised by an attacker. This activity can be associated with the **Multiple File Access Permission Changes**, **Multiple Failed File Access Permission Changes**, and **Abnormal File Access Permission Change** indicators.
Abnormal Active Directory (AD) Changes	If an attacker gains highly-privileged access to an Active Directory domain or domain controller, that access can be leveraged to access, control, or even destroy the entire forest. If a single domain controller is compromised and an attacker modifies the AD database, those modifications replicate to every other domain controller in the domain, and depending on the partition in which the modifications are made, the forest as well. Investigate abnormal changes conducted by admins and non-admins in AD to determine if they represent a possible true compromise to the domain. This activity can be associated with the **Abnormal Active Directory Change**, **Multiple Account Management Changes**, **Multiple User Account Management Changes**, and **Multiple Failed Account Management Changes** indicators.

Alert Type	Description
Sensitive User Status Changes	A domain or enterprise administrator account has the default ability to exercise control over all resources in a domain, regardless of whether it operates with malicious or benign intent. This control includes the ability to create and change accounts; read, write, or delete data; install or alter applications; and erase operating systems. Some of these activities trigger organically as part of the account's natural life cycle. Investigate these security sensitive user account changes, and determine if it is compromised. This activity can be associated with the **User Account Enabled**, **User Account Disabled**, **User Account Unlocked**, **User Account Type Changed**, **User Account Locked**, **User Password Never Expires Option Changed**, **User Password Changed by Non-Owner**, and **User Password Change** indicators.
Abnormal File Access	Monitor for abnormal file access to prevent improper access to confidential files and theft of sensitive data. By selectively monitoring file views, modifications and deletions, you can detect possibly unauthorized changes to sensitive files, whether caused by an attack or a change management error. This activity can be associated with the **Abnormal File Access Event** and **Multiple File Delete Events** indicators.
Non-Standard Hours	All authentication activity, malicious or not, appears as normal logons. Therefore, administrators should monitor unexpected authorized activity. The key is that attackers use these stolen credentials for unauthorized access, which may provide an opportunity for detection. When an account is being used for unusual activities, for example, authenticating an unusual number of times, the account may have been compromised. Use the indication of an abnormal activity time to determine if the account is taken over by an external actor. This activity can be associated with the **Abnormal File Access Time**, **Abnormal VPN Logon Time Abnormal Azure AD Logon Time**, **Abnormal Active Directory Change Time**, and **Abnormal Logon Time** indicators.
Credential Dumping	Credential dumping is the process of obtaining account login and password information, in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform lateral movement and access restricted information. This activity can be associated with the **Abnormal Process Created a Remote Thread in LSASS** indicator.

Alert Type	Description
Discovery & Reconnaissance	Discovery consists of techniques that allow the adversary to gain knowledge about the system and internal network. When attackers gain access to a new system, they must orient themselves to what they now have control of and what benefits operating from that system give to their current objective or overall goals during the intrusion. The operating system provides many native tools that aid in this post-compromise information-gathering phase. This activity can be associated with the **Abnormal Reconnaissance Tool Execute , Multiple Distinct Reconnaissance Tools Executed, Multiple Reconnaissance Tool Activities Executed** and **User Executed a Reconnaissance Tool Multiple Times** indicators.
PowerShell & Scripting	PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Attackers can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer. This activity can be associated with the **User Ran an Abnormal Process to Execute a Scripting Tool, Abnormal Process Executed a Scripting Tool, Scripting Tool Triggered an Abnormal Application, User Ran a Scripting Tool that Triggered an Abnormal Application, User Ran a Scripting Tool to Open an Abnormal Process** and **Scripting Tool Opened an Abnormal Process** indicators.
Registry Run Keys & Start Folder	Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. The program will be executed under the context of the user and will have the account's associated permissions level. Attackers can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Attackers may also use Masquerading to make the Registry entries look as if they are associated with legitimate programs. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level. This activity can be associated with the **Abnormal Process Modified a Registry Key Group** indicator.
Multiple Failed Authentications - External Access	As organizations increase their reliance on external authentication infrastructures, attackers may attempt to leverage these infrastructures to their advantage. Brute force techniques as well as more traditional password cracking methods like guesswork can be utilized to gain initial access. These activities can be associated with the **Multiple Failed Azure AD Authentications** and **Multiple Failed VPN Authentications** indicators.

Alert Type	Description
Abnormal Country	As organizations increase their reliance on external authentication infrastructures, attackers may attempt to leverage these infrastructures to their advantage. When devices or accounts are compromised as well as when credentials are wrongly shared, attackers may utilize them to gain initial access from an abnormal location. These activities can be associated with the **Abnormal Azure AD Logon Country** and **Abnormal VPN Logon Country** indicators.
Snooping User - Cloud Service Account	Snooping is unauthorized access to company data or data belonging to another person. Snooping can be as simple as the casual observance of an email on another person's computer. More sophisticated snooping uses software programs to remotely monitor activity on a computer or a cloud service account. This activity can be associated with the **Azure AD - Logon Attempts to Multiple Applications** indicator.
Abnormal Remote Application	Attackers may leverage compromised account details or devices to access remote applications that genuine end users do not frequently access to collect and even exfiltrate sensitive information. This activity can be associated with the **Azure AD - Abnormal Application** indicator.
Process Injection	Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. This activity can be associated with the **Abnormal Process Created a Remote Thread in a Windows Process** indicator.

Alert Types for Network Entities

Alert Type	Description
Phishing	Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. This activity can be associated with **Abnormal Country for SSL Subject**, and **Abnormal SSL Subject for JA3.** indicators.
Data Exfiltration	Data exfiltration is the unauthorized copying, transfer, or retrieval of data from a computer or server. Data Exfiltration is a malicious activity performed through various techniques, typically by cyber criminals over the Internet or other network. This activity can be associated with **Abnormal Traffic Volume Sent to Domain** and **Abnormal Traffic Volume Sent from JA3** indicators.

Alert Type	Description
Command & Control (C&C)	Command and control infrastructure can be leveraged by attackers as a communication channel between a compromised asset within the impacted network and an attacker-controlled server. Attackers may attempt to mask this malicious communication within regular network traffic; consequently, this activity can be associated with numerous network indicators such as **Abnormal Destination Port for JA3** and **High Number of IPs Contact a New SSL Subject**.

NetWitness UEBA Indicators

Indicators for Users

The following tables list indicators that display when a potentially malicious activity is detected for users.

Windows File Servers

Indicator	Alert Type	Description	
Abnormal File Access Time	Non-Standard Hours	A user has accessed a file at an abnormal time.	
Abnormal File Access Permission Change	Mass Permission Changes	A user changed multiple share permissions.	
Abnormal File Access Event	Abnormal File Access	A user has accessed a file abnormally.	
Multiple File Access Permission Changes	Mass Permission Changes	A user changed multiple file share permissions.	
Multiple File Access Events	Snooping User	A user accessed multiple file events.	
Multiple Failed File Access Events	Snooping User	A user failed multiple times to access a file.	
Multiple File Open Events	Snooping User	A user opened multiple files.	
Multiple Folder Open Events	Snooping User	A user opened multiple folders.	
Multiple File Delete Events	Abnormal File Access	A user deleted multiple files.	
Multiple Failed File Access Permission Changes	Mass Permission Changes	A user failed multiple attempts to change file access permissions	

Active Directory

Indicator	Alert Type	Description
Abnormal Active Directory Change Time	Non-Standard Hours	A user made Active Directory changes at an abnormal time.
Abnormal Active Directory Object Change	Abnormal AD Changes	A user made Active Directory attribute changes abnormally.
Multiple Group Membership Changes	Mass Changes to Groups	A user made multiple changes to groups successfully.
Multiple Active Directory Object Changes	Abnormal AD Changes	A user made multiple Active Directory changes successfully.
Multiple User Account Changes	Abnormal AD Changes	A user made multiple sensitive Active Directory changes successfully.
Multiple Failed Account Changes	Abnormal AD Changes	A user failed to make multiple Active Directory changes.
Admin Password Changed	Admin Password Change	The password of an admin was changed.
User Account Enabled	Sensitive User Status Changes	An account of a user was enabled.
User Account Disabled	Sensitive User Status Changes	An account of a user was disabled.
User Account Unlocked	Sensitive User Status Changes	An account of a user was unlocked.
User Account Type Changed	Sensitive User Status Changes	The type of user was changed.
User Account Locked	Sensitive User Status Changes	An account of a user was locked.
User Password Reset	Sensitive User Status Changes	The password of a user was reset.
User Password Never Expires Option Changed	Sensitive User Status Changes	The password policy of a user was changed.

Logon Activity

Indicator	Alert Type	Description
Abnormal Remote Computer	Abnormal Computer Access	A user accessed a remote computer abnormally.

Indicator	Alert Type	Description
Abnormal Logon Time	Non-Standard Hours	A user logged on at an abnormal time.
Abnormal Computer	User Login to Abnormal Host	A user attempted to access a computer abnormally.
Multiple Successful Authentications	Multiple Logons by User	A user logged on multiple times.
Multiple Failed Authentications	Multiple Failed Logons	A user failed multiple authentication attempts.
Logon Attempts to Multiple Source Computers	User Logged into Multiple Hosts	A user attempted to log on from multiple computers.

Process

Indicator	Alert Type	Description
Abnormal Process Created a Remote Thread in LSASS	Credential Dumping	An abnormal process was created into the LSASS process.
Abnormal Reconnaissance Tool Executed	Discovery and Reconnaissance	An abnormal process was executed.
Abnormal Process Executed a Scripting Tool	PowerShell and Scripting	An abnormal process executed a scripting tool.
Abnormal Process Executed a Scripting Tool	PowerShell and Scripting	An abnormal process was triggered by a scripting tool.
Scripting Tool Triggered an Abnormal Application	PowerShell and Scripting	An abnormal process was opened by a scripting tool.
Abnormal Process Created a Remote Thread in a Windows	PowerShell and Scripting	An abnormal process was injected into a known windows process .
Multiple Distinct Reconnaissance Tools Executed	Discovery and Reconnaissance	Multiple reconnaissance tools were executed in an hour.
Multiple Reconnaissance Tool Activities Executed	Discovery and Reconnaissance	Multiple reconnaissance tool activities were executed in an hour.
User Ran an Abnormal Process to Execute a Scripting Tool	PowerShell / Scripting	An abnormal process executed a scripting tool.
User Ran a Scripting Tool that Triggered an Abnormal Application	PowerShell / Scripting	A scripting tool was executed that triggered an abnormal application.
User Ran a Scripting Tool to Open an Abnormal Process	PowerShell / Scripting	A scripting tool was executed to open an abnormal process.

Registry

Indicator	Alert Type	Description
Abnormal Process Modified a Registry Key Group	Registry Run Keys	An abnormal process modified a service key registry.

Indicators for Network Entities

The following tables list indicators that display when a potentially malicious activity is detected for JA3 and SSL Subject entities.

> **Note:** Indicators are for JA3, and in some instances the JA3 hash can be mapped to more than one client application.

Indicator	Entity Type	Alert Type	Description
Abnormal Traffic Volume Sent from IP to SSL Subject	SSL Subject	Data exfiltration	An IP address in the organization sent an unexpectedly high amount of data to an SSL Subject.
Abnormal Traffic Volume Sent from IP to Domain	SSL Subject	Data exfiltration	An IP address in the organization sent an unexpectedly high amount of data to a domain and SSL Subject.
Abnormal Traffic Volume Sent from IP to Organization	SSL Subject	Data exfiltration	An IP address in the organization sent an unexpectedly high amount of data to an organization and SSL Subject.
Abnormal Traffic Volume Sent from IP to Port	SSL Subject	Data exfiltration	An IP address in the organization sent an unexpectedly high amount of data to a port and SSL Subject.
Abnormal Traffic Volume Sent to SSL Subject	SSL Subject	Data exfiltration	An unexpectedly high amount of data was sent to an SSL Subject.
Abnormal Traffic Volume Sent to Domain	SSL Subject	Data exfiltration	An unexpectedly high amount of data was sent to a domain and SSL Subject.
Abnormal Traffic Volume Sent to Port	SSL Subject	Data exfiltration	An unexpectedly high amount of data was sent to a port and SSL Subject.
Abnormal Traffic Volume Sent to Organization	SSL Subject	Data exfiltration	An unexpectedly high amount of data was sent to an organization and SSL Subject.
Abnormal Traffic Volume Sent from JA3	JA3	Data exfiltration	Abnormal number of bytes sent from JA3 .

Indicator	Entity Type	Alert Type	Description
High Number of IPs Use JA3	JA3	C&C	An abnormally high number of IPs use JA3.
Abnormal SSL Subject for Source Netname	SSL Subject and JA3	Phishing	A source netname contacted an abnormal SSL Subject.
Abnormal Domain for Source Netname	SSL Subject and JA3	Phishing	A source netname contacted an abnormal domain
Abnormal Destination Port for Source Netname	SSL Subject and JA3	C&C	A source netname contacted an abnormal destination port.
Abnormal Organization for Source Netname	SSL Subject and JA3	Phishing	A source netname contacted an abnormal organization.
Abnormal Country for SSL Subject	SSL Subject and JA3	Phishing	An SSL Subject was contacted with an abnormal destination country.
Abnormal Destination Port for SSL Subject	SSL Subject and JA3	C&C	An SSL Subject was contacted through an abnormal destination port.
Abnormal Time for SSL Subject	SSL Subject and JA3	Non-Standard Hours	An SSL Subject was contacted at an abnormal time.
Abnormal Destination Port for Domain	SSL Subject and JA3	C&C	A domain was accessed through an abnormal destination port.
Abnormal Destination Port for Organization	SSL Subject and JA3	C&C	An organization was accessed through an abnormal destination port.
Abnormal Time for JA3	SSL Subject and JA3	Non-Standard Hours	JA3 was used at an abnormal time.
Abnormal JA3 for Source Netname	SSL Subject and JA3	C&C	A source netname utilized an abnormal client application.
Abnormal SSL Subject for JA3	SSL Subject and JA3	Phishing	JA3 contacted an abnormal SSL Subject.
Abnormal Domain for JA3	SSL Subject and JA3	Phishing	JA3 contacted an abnormal domain.
Abnormal Destination Port for JA3	SSL Subject and JA3	C&C	JA3 contacted an abnormal destination port.
High Number of IPs Contact a New SSL Subject	SSL Subject	C&C	High number of IPs contacted SSL Subject.
High Number of IPs Contact a New Domain	SSL Subject	C&C	High number of IPs contacted a new domain.

Indicator	Entity Type	Alert Type	Description
High Number of IPs Contact a New Organization	SSL Subject	C&C	High number of IPs contacted a new organization.
High Number of IPs Contact a New Port	SSL Subject	C&C	High number of IPs contacted a new port.
Abnormal Traffic Volume Sent from an IP to a New SSL Subject	SSL Subject	Data Exfiltration	Abnormal number of bytes sent from an IPs to an SSL Subject.
Abnormal Traffic Volume Sent from an IP to a New Domain	SSL Subject	Data Exfiltration	Abnormal number of bytes were sent an IP to a domain.
Abnormal Traffic Volume Sent from an IP to a New Port	SSL Subject	Data Exfiltration	Abnormal number of bytes were sent from an IP to a port.
Abnormal Traffic Volume Sent from an IP to a New Organization	SSL Subject	Data Exfiltration	Abnormal number of bytes were sent from an IP to an organization.
Abnormal Traffic Volume Sent to a New SSL Subject	SSL Subject	Data Exfiltration	Abnormal number of bytes were sent to a SSL Subject. n
Abnormal Traffic Volume Sent to a New Domain	SSL Subject	Data Exfiltration	Abnormal number of bytes were sent to a new domain.
Abnormal Traffic Volume Sent to a New Port	SSL Subject	Data Exfiltration	Abnormal number of bytes were sent to a new port.
Abnormal Traffic Volume Sent to a New Organization	SSL Subject	Data Exfiltration	Abnormal number of bytes were sent to an organization for an SSL Subject.
Abnormal Traffic Volume Sent from a New JA3	JA3	Data Exfiltration	Abnormal number for bytes were sent to JA3.

Access NetWitness UEBA

Note: To access the NetWitness UEBA service and Users tab, you must be assigned to either the UEBA_Analyst role or Administrators role. For information about how to assign these roles, see the "How Role-Based Access Control Works" topic in the *System Security and User Maintenance Guide*

To access NetWitness UEBA, log in to NetWitness and do one of the following:

1. Go to **Users** > **Overview** to view the NetWitness UEBA feature displayed.
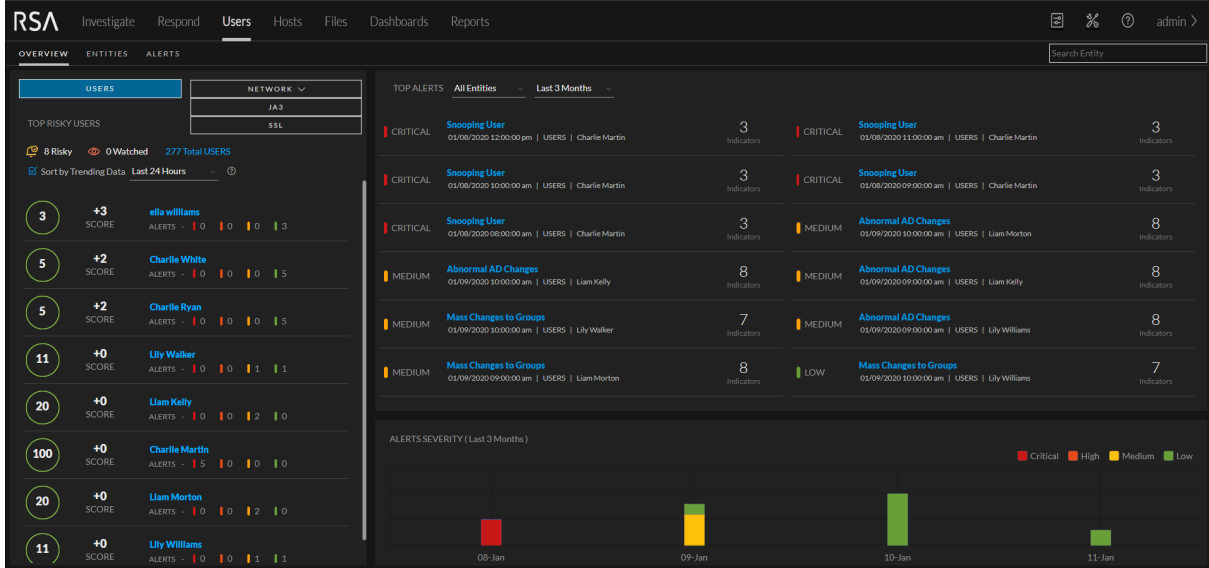
2. Click ❭ in the **Top Risky Users** panel displayed on the Springboard to view the **Users** tab.
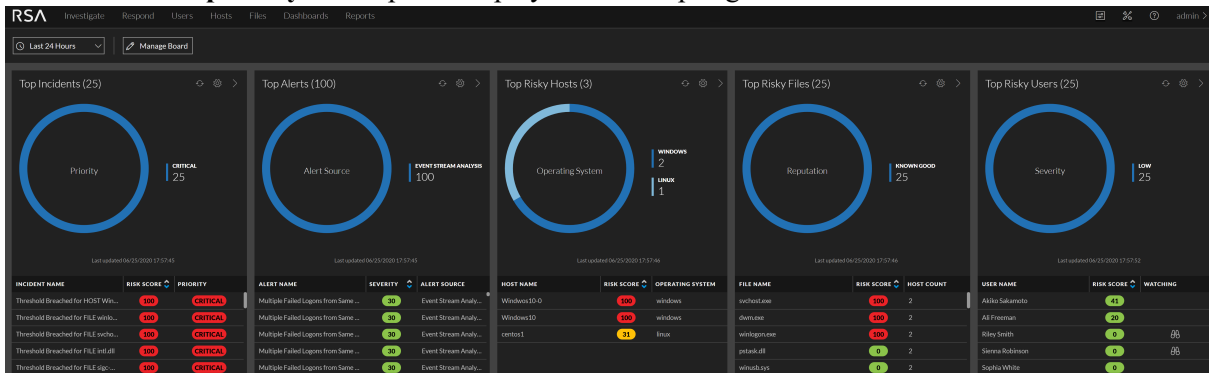
You can choose a dark or a light theme for the view. For more information, see the "Choose the Appearance of NetWitness" topic in the *RSA NetWitness Getting Started Guide*.

UEBA Licensing

You must alo ensure that you have NetWitness UEBA licensing configured. For information about NetWitness UEBA licensing, see the "User and Entity Behavior Analytics License" topic in the *Licensing Management Guide*.

Investigate High-Risk Entities

An entity score is built based on the alert score and the alert severity. Using the entity score, you can identify entities that require immediate attention, perform deeper investigation, and take required action. You can identify high-risk entities from either the **Overview** tab or the **ENTITIES** tab.

The following figure is an example of top ten High-Risk entities in the **Overview** tab.
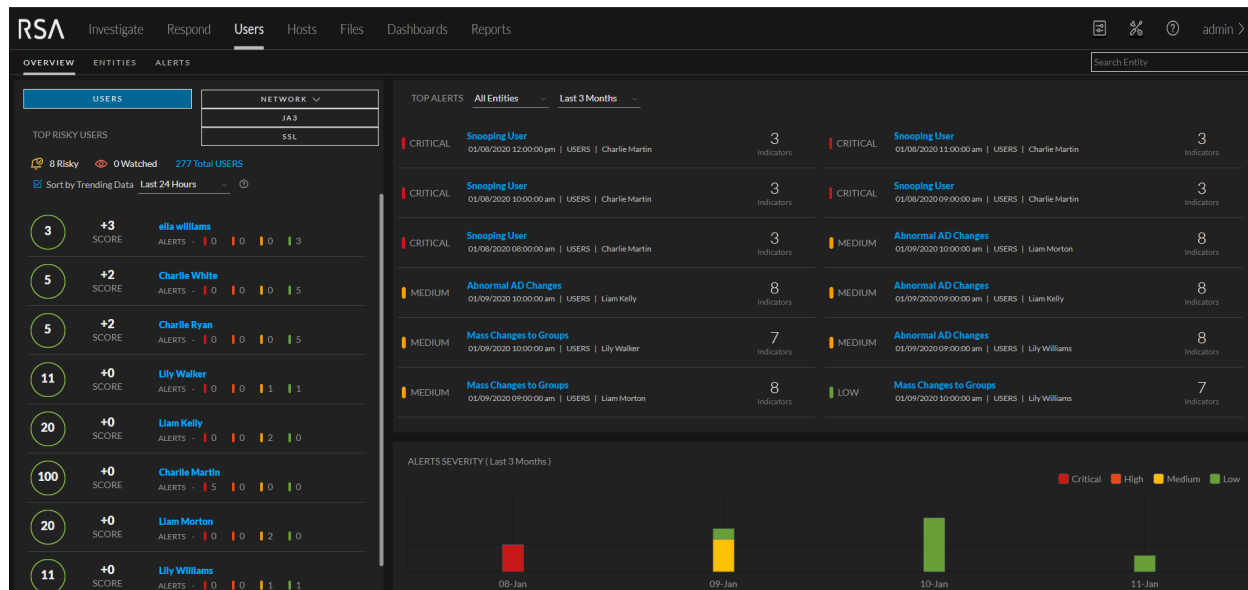
The following figure is an example of all the risky entities in your environment in the **ENTITIES** tab.
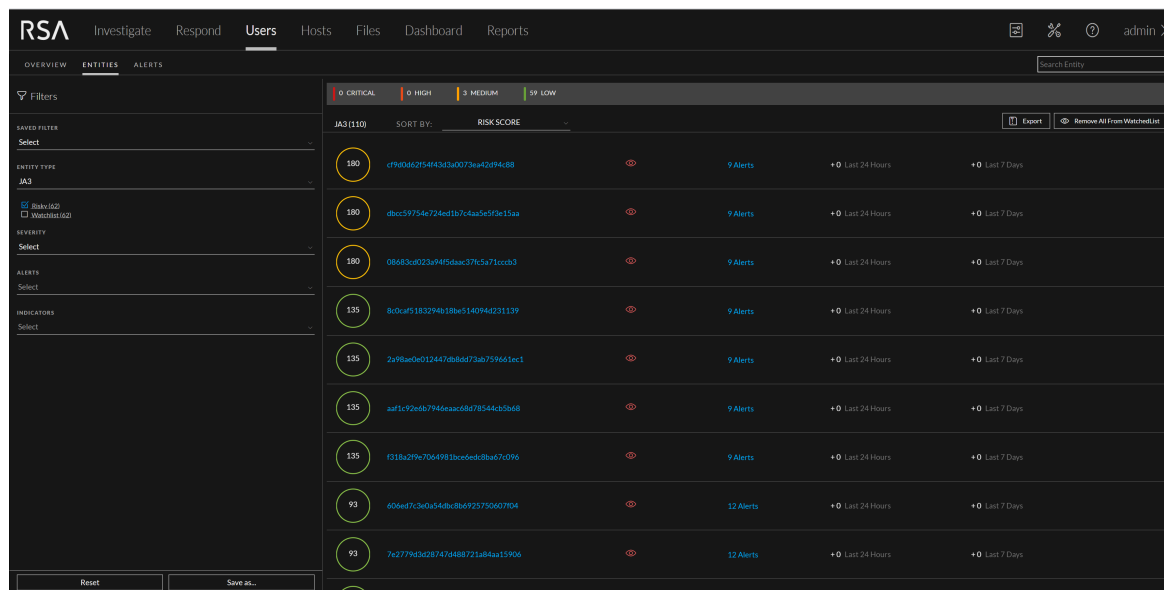
The following is a high-level process to investigate high-risk entities in your environment.

1. Identify high-risk entities. You can identify high-risk users using the following ways:

   - The **Overview** tab shows the top ten risky entities in your environment. From the listed entities identify the entities with a critical severity or entity score more than 100.

   - The **ENTITIES** tab shows all the risky entities in your environment, you can sort by Risk Score (default), Trending Data Last Day or Last Week (marked with +), Name, Alerts. Identify how many entities are marked Critical, High and Medium or based on the forensic investigation, identify malicious entity behavior and build use-case driven target entity lists using behavioral filters. Additionally, you can also use different types of filters (Risky or Watchlist) to identify targeted group of high-risk entities.

   > **Note:** The investigation should mostly focus on Critical, High and Medium severities. Low scoring users are not typically worth much investigation.

   Hover over the number of alerts associated with the risky entities to quickly see what the alerts are and determine if there is a good mix.

   For more information, see the Identify High-Risk Entities topic.

2. In the **User Profile** view, investigate the alerts and indicators of the user.

   a. Review the list of alerts associated with the user and the alert score for each alert, sorted by severity.

   b. Expand the alert names to identify a threat narrative. The strongest contributing indicator determines the alert's name that suggests why this hour is flagged.

   c. Use the alert flow timeline to understand the abnormal activities.

   d. Review each indicator associated with the alert to see the details about the indicator, including the timeline in which the anomaly occurred. Also, you can further investigate the incident using external resources such as SIEM, network forensics, directly reaching out to the user or a managing director and so on.

   For more information, see the Begin an Investigation of High-Risk Entity topic.

3. On completion of the investigation, you can record your observation as follows:

   a. Specify if an alert is not a risk.

   b. Save the behavioral profile for the use case found in your environment.

   c. If you want to keep a track of user activity, you can add users to the watchlist, and watch user profile.

   For more information, see the Take Action on High-Risk Users topic.

Identify High-Risk Entities

You can identify high-risk user in your environment in the following ways:

- View top five high-risk entities
- View all the high-risk entities

- View users of a specific group

- View users and other entities based on forensic investigation

View Top Ten Risky Entities

In the **OVERVIEW** tab, you can view the list of top five high-risk entities in your environment along with the risky score.

To view the top risky entities:

Log into **NetWitness** and go to **Investigate** > **ENTITIES**.
The Overview tab is displayed with the high-risk users displayed in the High Risk Users tab, and high-risk SSL and hight-risk JA3 are displayed under the Network tab.

View All High-Risk Entities

In the **Network** tab, you can view the list of all the high risk users in your environment along with the user score and total number of alerts associated with the users.

To view all high-risk users:

1. Log into **NetWitness** and go to **Investigate** > **ENTITIES**.

   The Overview tab is displayed.

2. Click **ENTITIES** tab.

The list of all high-risk entities are displayed.

View Entities of Specific Group

In the **Network** tab, you can use different types of filters to identify targeted group of high-risk entity.

To view users of specific group:

1. Log into **NetWitness** and go to **Investigate** > **ENTITIES**.

   The Overview tab is displayed.

2. Click the **ENTITIES** tab.

3. In the **Filters** panel, do any of the following:

   - **Risky Entities**: To view all the risky entities in your environment, select **Risky** . By default, risky entities along with their risky score are displayed.

   - **Watchlist** : To view the list of entities that you added to the watchlist to monitor for specific

changes, select **Watchlist**.

> **Note:** You can view users of one or more group by selecting one or more filters. For example, if you want to view the list of admin users who are risky users, select the **Admin Users** and **Risky Users** filters.

View Entity Based on Forensic Investigation

In the **ENTITIES** tab, you can use Alert Types and Indicators which are behavioral filters to view high-risk users based on forensic investigation. For more information on forensic investigation, see *Forensic Workflow* in the [Introduction](#) topic.

To view users based on specific forensic investigation:

1. Log into **NetWitness** and go to **Investigate** > **ENTITIES**.

   The Overview tab is displayed.

2. Click **ENTITIES** tab.

3. To create a behavioral filter using alert types, select one or more alerts in the **ALERTS** drop-down list.

4. To create a behavioral filter using indicators, select one or more indicators in the **INDICATORS** drop-down list.

5. To filter the result for JA3 entity, select JA3 from the **ENTITY TYPE** drop-down list.

> **Note:** You can select combination of one or more alert types and indicators to create a behavioral filter based on your requirement. For example, to monitor abnormal access to confidential files and theft of sensitive data, you can create a behavioral filter with Alert Types = **Data Exfiltration** and Indicators = **Abnormal JA3 for Source Netname (3 JA3)**.

To save these behavioral filters as favorites for future investigation, click **Save as...**.

To delete the filters click **Reset Filters**.

Similarly, you can view the results for the SSL entity based on forensic investigation.

Begin an Investigation of High-Risk Entity

After identifying the high-risk entities, you can begin the investigation of high-risk entities.

To investigate high-risk entities:

1. Log into **NetWitness** and go to **INVESTIGATE** > **ENTITIES**.

   In the **Overview** tab, select **ENTITIES** tab, select an entity from the **NETWORK** drop-down to investigate. For example, if you select **Network** > **JA3**, all the JA3 high-risk entities will be displayed. Also, can sort the results by selecting the **Sort by Trending Data** checkbox. If you select this option, the data will be sorted by the Entity score (marked with +) that changed in the past 24 hours or in the past one week. By default, the result is sorted by the Entity risk score.

2. To further investigate the alert of the entity, click an alert in the **High Risk JA3** panel. The following information is displayed:

   - The alert name

   - The timeframe of the alert (Hourly or Daily)

   - The severity level icon

   - The contribution to the entity score value (for example, 20)

   - The data sources for the alert (for example, TLS)
     The middle panel is the Alert Flow panel. This panel provides a timeline of events that are related to the formation of the alert. The timeline of events can help to determine if the alert is an actual

risk.
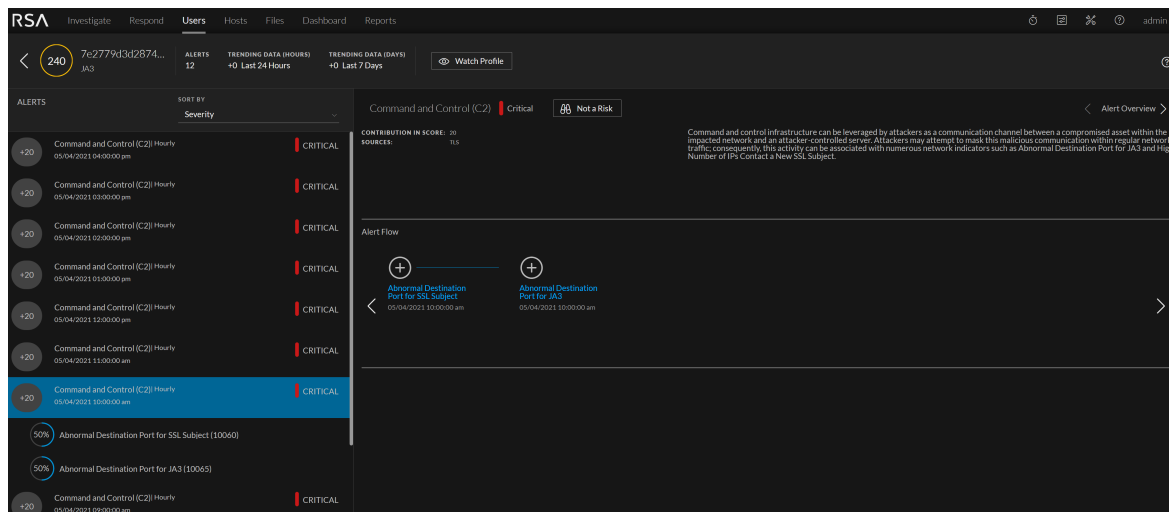
3. To investigate the indicators associated with an alert for an entity, in the **High Risk** panel, select an alert and then select an indicator. The following information is displayed:

    - The indicator name and a description of the indicator type

    - Contribution to Alert

    - The anomaly values

    - The data source of the events found in the indicator
      The central panel display changes depending on which indicator is selected.
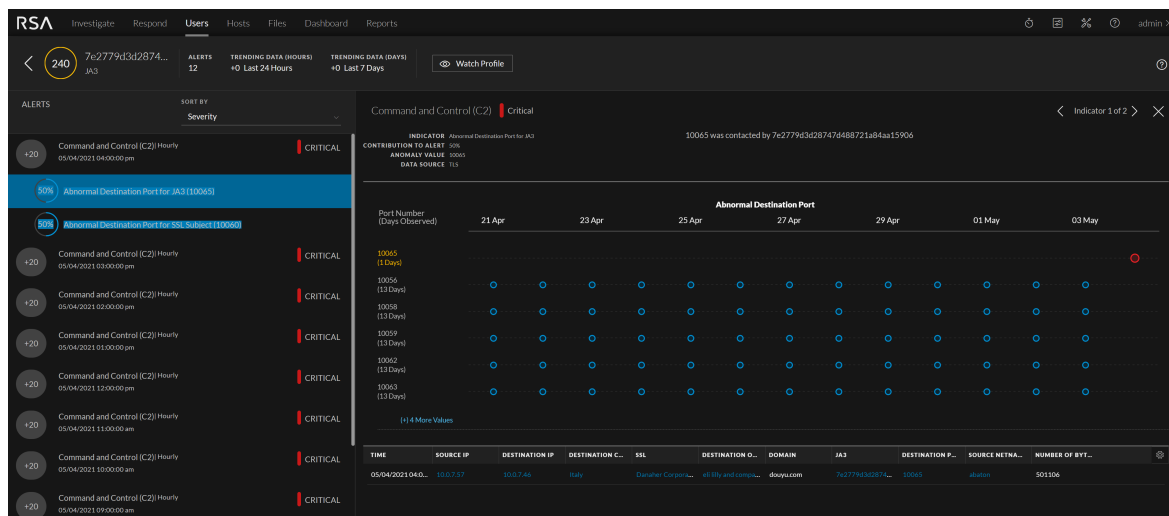
> **Note:** You can investigate a high risk SSL entity using the above procedure.

For more information on how to read the indicator charts, see Reading an Indicator Chart topic.

Take Action on High-Risk Users

After investigation, you can take action on the risky users to reduce or prevent further damage caused by malicious attackers in your organization. You can take any of the following actions:

- Specify if the alert is not risky

- Save the behavioral profile for the use case found in your environment

- Add users to the watchlist, and the watch user profile, if you want to keep a track of the user activity

Specify that an alert is not risky.

If and alert is not a risk, you can mark it so that the user score for the user is automatically reduced.

To specify if the alert is not risky:

1. Log into **NetWitness** and go to **Investigate** > **ENTITIES**.

2. Take action on the users from any of the following tabs:

   a. In the **OVERVIEW** tab, in the **High Risk Users** panel, select a user and click either on the username or on the user score.

   b. In the **ENTITIES** tab, select a user and click on the username.
      The User Profile view is displayed.

3. If the alert is not a risk, you can specify by clicking **Not a Risk**.

When an alert is marked as **Not a Risk**, the user score is reduced automatically.

Save Behavioral Profile

The combination of the alert types and indicators you select during the forensics investigation is a behavioral profile. You can save the behavioral profile, so you can monitor this use case in future.

For example, if your organization is attacked and the attackers penetrated by brute forcing user accounts, you can select filters using the brute force alert type. This can be saved as favorite. You can proactively monitor for future brute force attempts. To do so, you can click the favorite to see if new users were subjected to this type of attack.

To save a behavioral profile:

1. Log into **NetWitness** and go to **Investigate** > **ENTITIES**.

   The Overview tab is displayed.

2. Click the **Users** tab.

3. In the **Filters** panel, select the alert in the **Alert Type** drop-down and Indicators in the **Indicators** drop-down.

4. Click **Save to Favorites**.
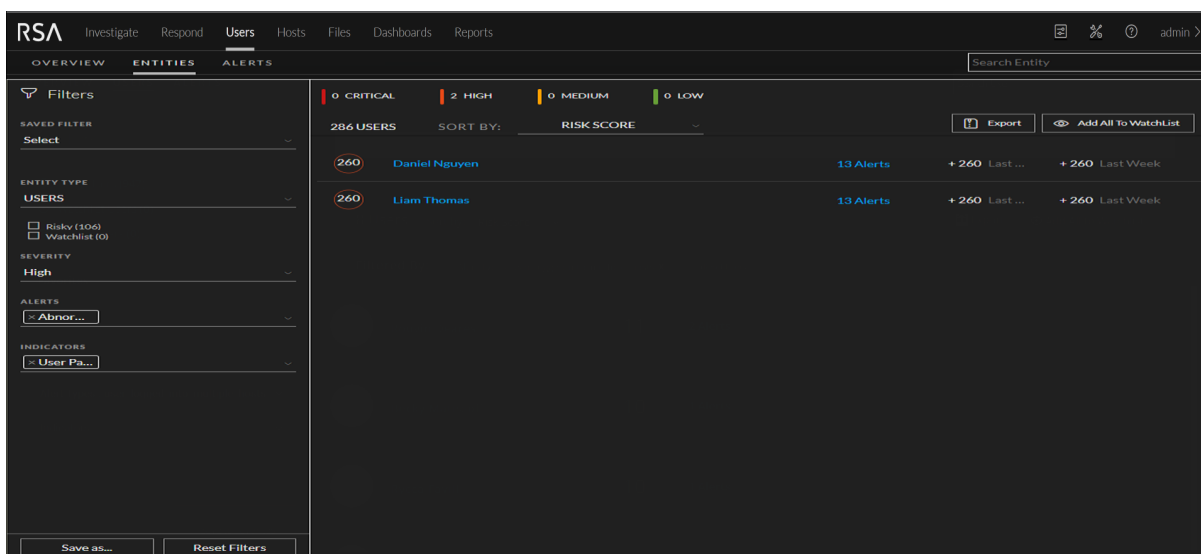
5. In the **Save Filter** dialog, enter the name of the filter and click **OK**.
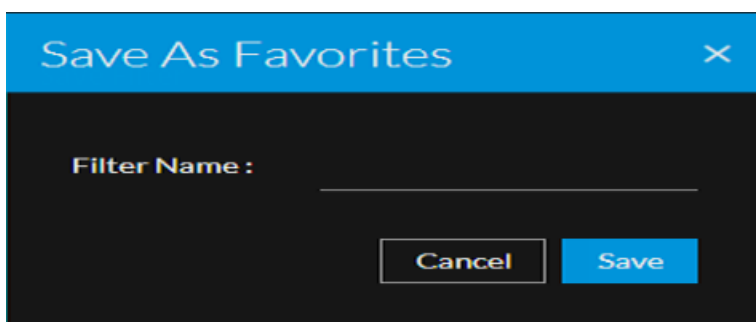
   The behavioral profile is saved and displayed in the Favorites panel. You can click on the profile in the Favorites to monitor the users.

Add All Users to the Watchlist

If you want to keep track of users with recent activity but do not want to follow up with an immediate investigation, you can add the users to the watchlist and revisit over time to see if the risk score is elevated.

To add all users to the watchlist:

1. Log into **NetWitness** and go to **Investigate** > **ENTITIES**.
   The Overview tab is displayed.

2. Select the **ENTITIES** tab.

3. Select the users of specific categories using filters.

4. Click **Add All to Watchlist**.

The list of users are added to the watchlist.

Watch Profile

The watch user profile is a list of users that you want to monitor for potential threats. The watch user profile marks a user so that the users can be quickly referenced on the dashboard. This is essentially a bookmark to monitor suspicious users.

To watch user profile:

1. Log into **NetWitness** and go to **Investigate** > **ENTITIES**. Do any of the following:

   a. In the **Overview** tab, under **High Risk Users** panel, select a user and click on either the username or the user score.

   b. In the **Users** tab, select a user and click the username.
       The User Profile view is displayed.

2. Click **Watch Profile** in the upper right corner of the User Profile.
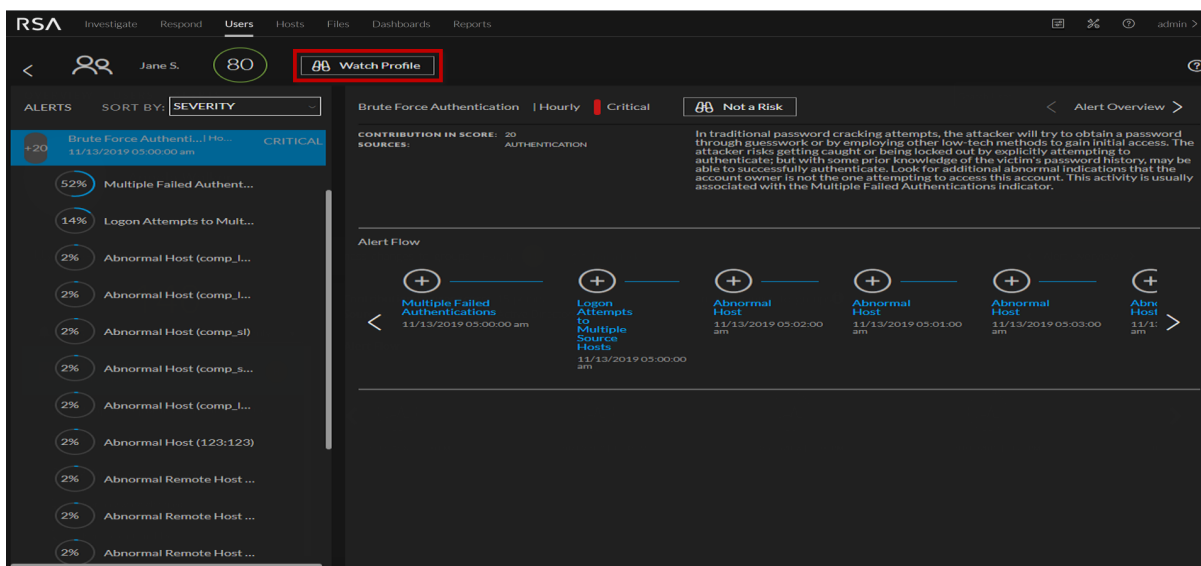
The user is added to the watchlist.

Export a list of High-Risk Users

You can export a list of all users and their scores in a .csv file format. You can use this information to compare with other data analysis tools like tableau, powerbi, and zeppelin.

To export a list of high-risk users:

1. Go to **INVESTIGATE** > **Users**.

   The Overview tab is displayed.

2. Select the **Users** tab.

3. Click **Export**.
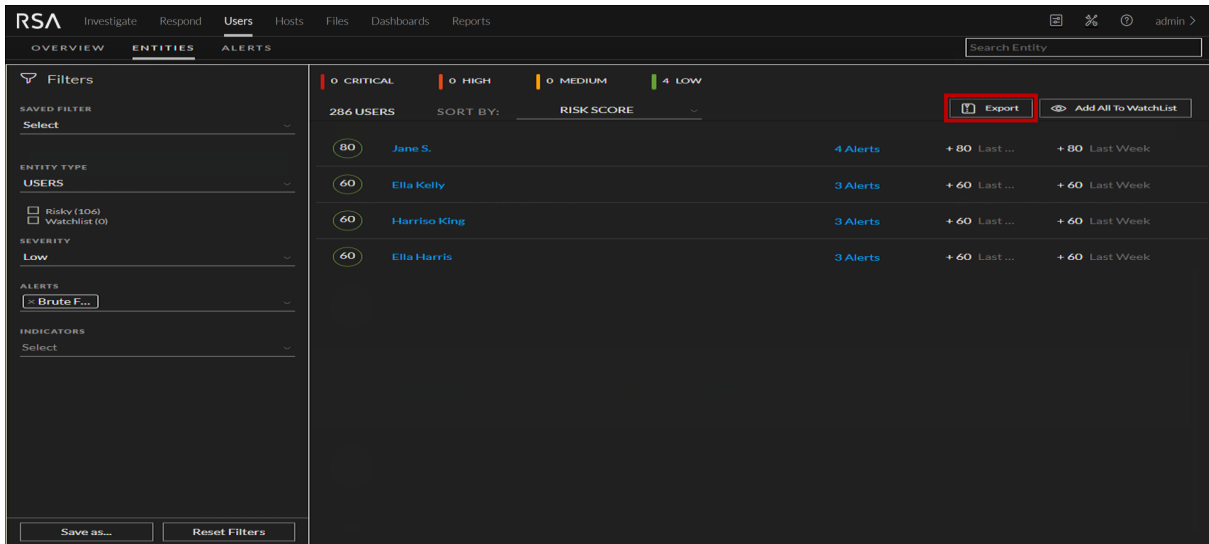
The list of all users and the associated user score is downloaded in the .csv file format.

Investigate Top Alerts

Anomalies that are found as incoming events are compared to the baseline and compiled into hourly alerts. Relatively strong deviations from the baseline, together with a unique composition of anomalies, are more likely to get a higher alert score.

You can quickly view the most critical alerts in your environment, and start investigating them from either the OVERVIEW tab or the ALERTS tab. The following figure is an example of top alerts in the OVERVIEW tab. The alerts are listed in order of severity and the number of users who generate the alerts.
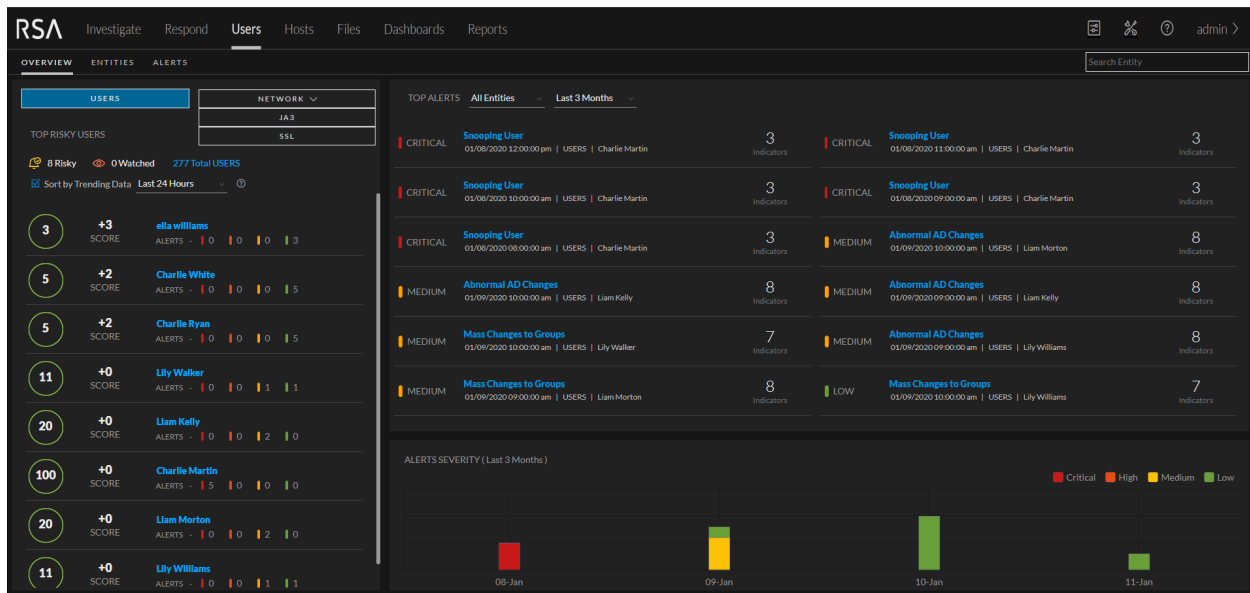
To investigate an alert on this page, click an alert in the **Top Alerts** section.

The following figure shows details about the event that caused the alert, and the time frame in which it occurred.
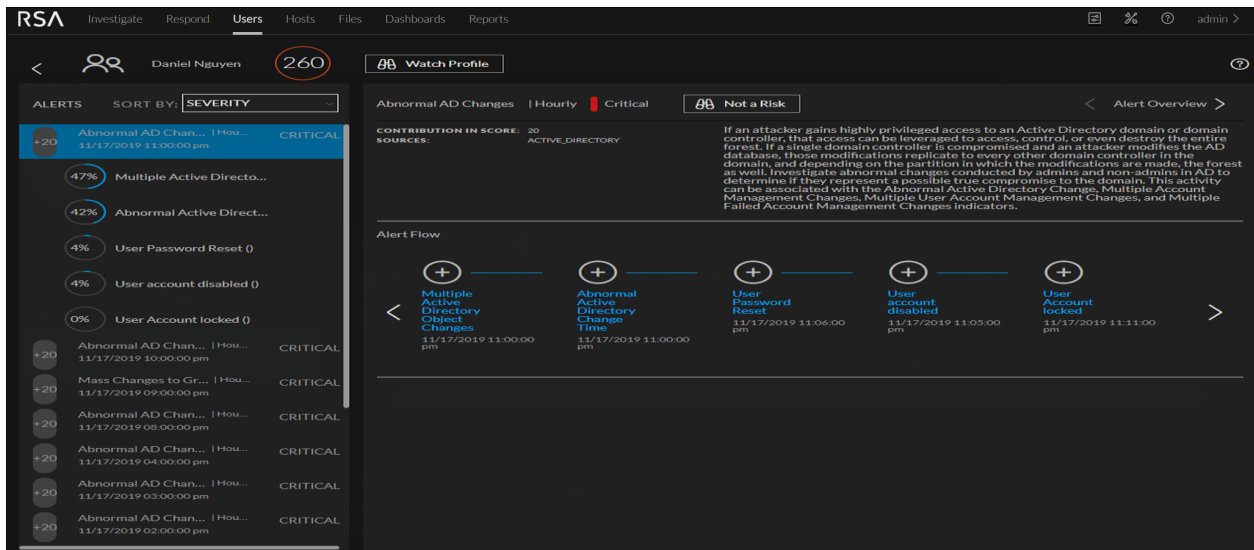
From the Alerts Severity panel at the bottom of the Overview tab, you can click on a bar in the graph to review top alerts in the ALERTS tab. The following figure shows the top alerts listed in the Alerts tab.
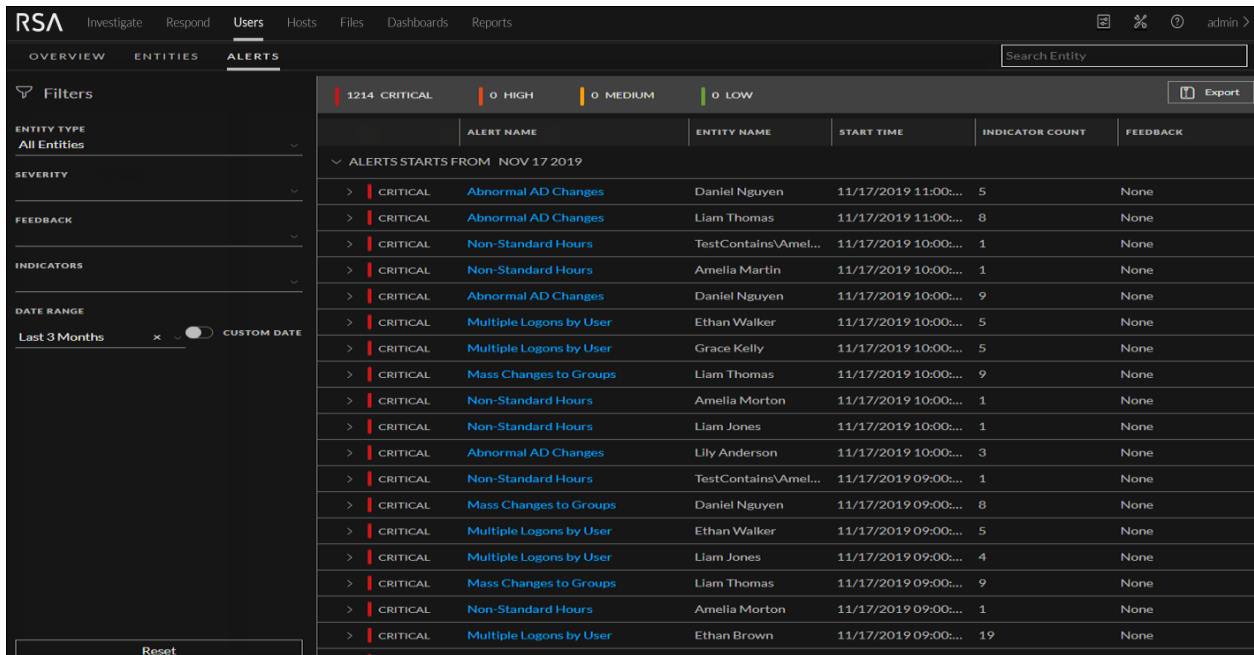
Investigating alerts is particularly useful when you want to focus on a timeframe in which you believe your systems were compromised. You can view forensic information based on a timeframe and gather detailed information about events that occurred during that time in the Alerts tab.
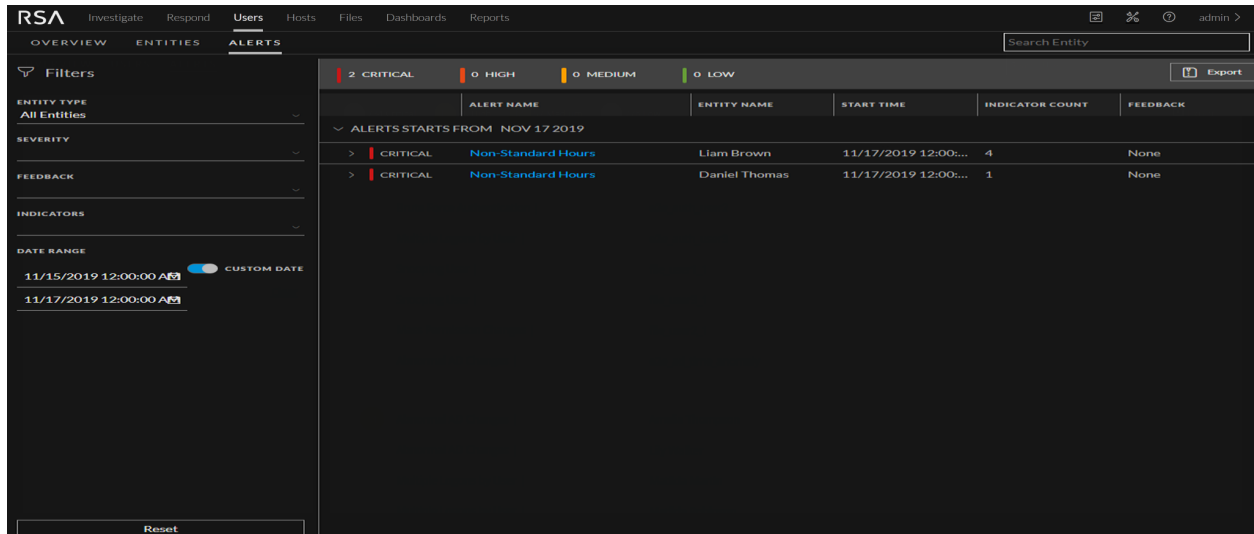
Begin an Investigation of Critical Alerts

You can begin your investigation of critical alerts in the following ways:
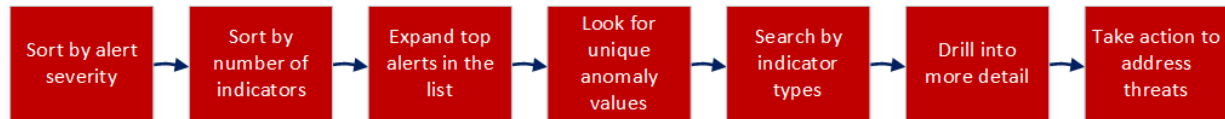
1. On the Overview tab, look at the ALL ALERTS.
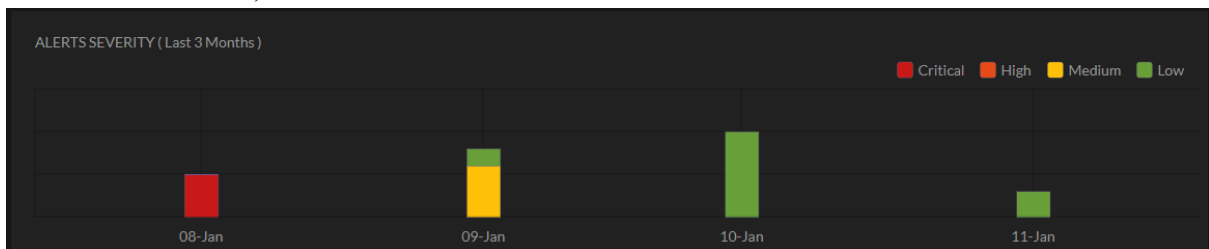
Is there an even distribution of alerts or are there a few days when there was a noticeable spike? A spike could indicate something suspicious like malware. Make a note of those days so you can inspect the alerts (the bar from the chart links directly to the alerts for that specific day).

2. In the Alerts tab, you can view the indicator count:

To identify users with the highest number of alerts, more indicators help illustrate more insights and provide a more rigid timeline that you can follow.

3. Expand the top alerts in the list:

• Look for alerts that have varied data sources. These show a broader pattern of behavior.

• Look for a variety of different indicators.

• Look for indicators with high numeric values, specifically for high values that are not indicative of a manual activity (for example, a user accessed 8,000 files).

4. Look for unique Windows event types that users do not typically change as these can indicate suspicious administrative activity.

5. Search by indicators.
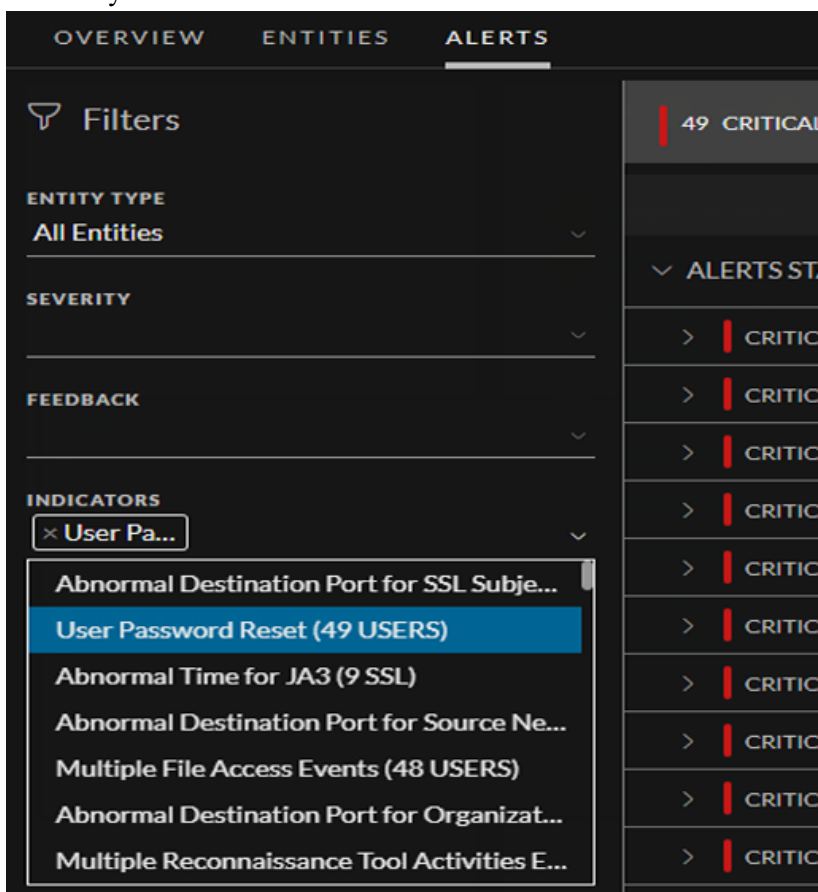
The list shows the number of alerts raised that contain each indicator.

- Look for the top volume indicators; filter by an indicator and review by user to find users who experienced the highest number of these indicators.

- In general, you can ignore time-based alerts (for example, Abnormal Logon Time) as these are very common. However, they provide good context when combined with higher interest indicators.

6. Drill into more detail:

- Leverage alert names to begin establishing a threat narrative. Use the strongest contributing indicator that usually determines the alert's name to begin explaining why this user is flagged.

- Use the timeline to layout the activities found and try to understand the observed behaviors.

- Follow up by reviewing each indicator and demonstrating the supporting information, in the form of graphs and events, that can help you verify an incident. Suggest possible next stages of investigation using external resources (for example, SIEM, network forensics, and directly reaching out to the user, or a managing director).

- Conclude the investigation by prompting for feedback and leaving a comment.

7. Take action to address threats determined by the investigation of alerts. For more information, see Take Action on High-Risk User or Network Entity .

The following topics explain various ways to investigate alerts.

- Filter Alerts
- Investigate Events
- Manage Top Alerts
- View NetWitness UEBA Metrics in Health and Wellness

Filter Alerts

You can filter alerts displayed in the Alerts tab by severity, feedback, entity, indicators, and date range.

1. Go to **Users** > **Alerts**.
   The Alerts tab is displayed.
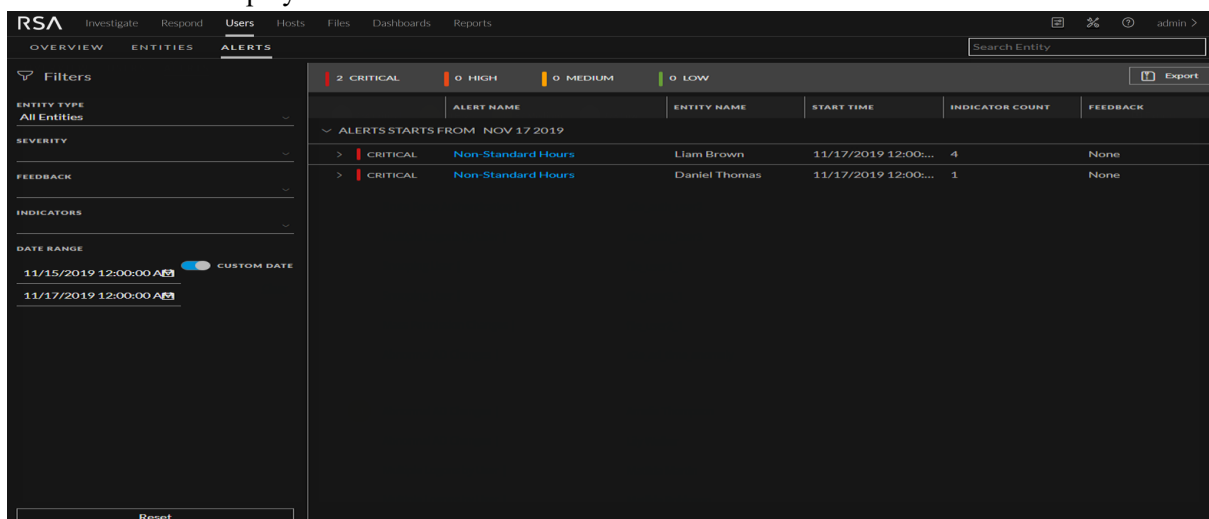
2. To filter by severity, click the down arrow under **Severity** in the **Alerts Filters** panel, and select any one option. The options are Critical, High, Medium, and Low.

3. To filter by feedback, click the down arrow under **Feedback**, and select any one option. The options are None, and Rejected.

4. To filter by entity, click the down arrow under **Entity Type**, and select any one option. The options are All Entities, Users, JA3, and SSL.

5. To filter by date range,

   - Click the down arrow under **Date Range** and select any one option. The Options are Last 7 Days, Last 2 Weeks, Last 1 Month, and Last 3 Months.

   - Select **Custom Date** under **Date Range**. In the **Start Date**, select the start range date range, and in the **End Date** select the end range date that you want the investigate.

The alerts are displayed in the right panel according to the filter you selected. To reset filters, in the bottom of left panel, click **Reset**.

Investigate Events

You can view all alerts and indicator associated with a user or network entity in the User Profile view.

In the events table, you can find all events contributed to the specific indicator for the specific user or network entity.

For example, you can further investigate on events by clicking on a username or a network entity that pivots to **Investigate** > **Events**. In the Events view, you can see the list of events that occurred on that day for the specific user or network entity. By default, the time range is set to one hour. You can change the time range.

In case of Endpoint Indicators, you can pivot to **Host Details** view and can have deeper insight about that host. And, pivot to **Analyze Process** view for detailed investigation on the process for that event for that week as the time range is set to seven days. By default, the time range is set to seven days however, it can be customized.

To view the events:

1. Go to **Users** > **Alerts**.

2. Under **Filters**, select the **Entity Type**.
   The indicators are displayed, along with the anomaly value, data source, and start time.
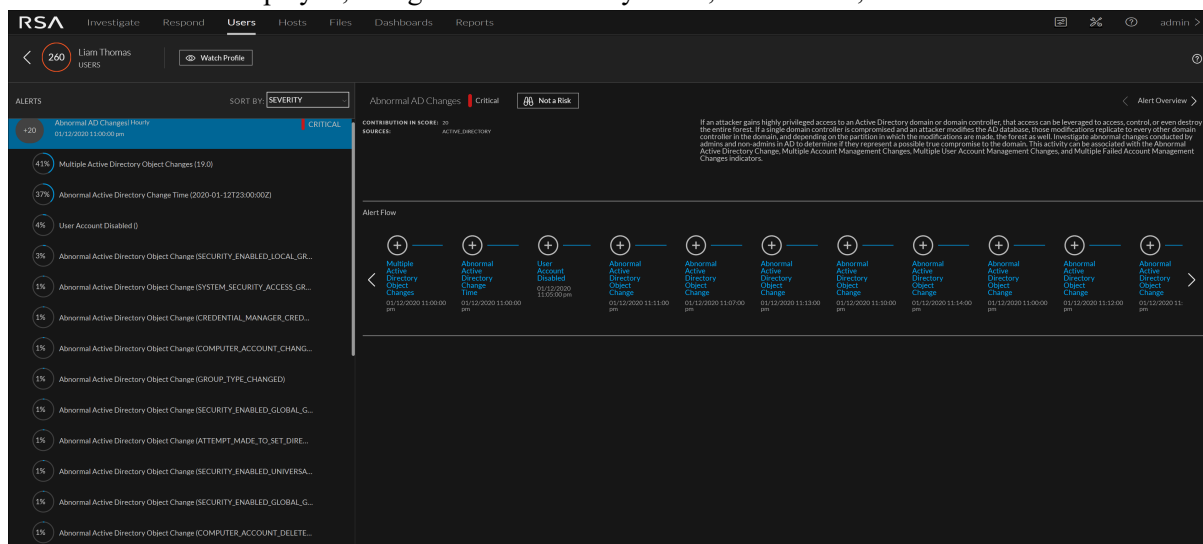
3. Click an alert name, and under **Alert Flow**, click the ⊕ icon.
   A graph is displayed that shows details about a specific indicator, including the timeline in which the anomaly occurred and the user associated with the indicator. The following figure shows an example of a graph. The type of graph can vary, depending on the type of analysis performed by NetWitness

UEBA. For more information, see [User or Network Entity Profile View](#).
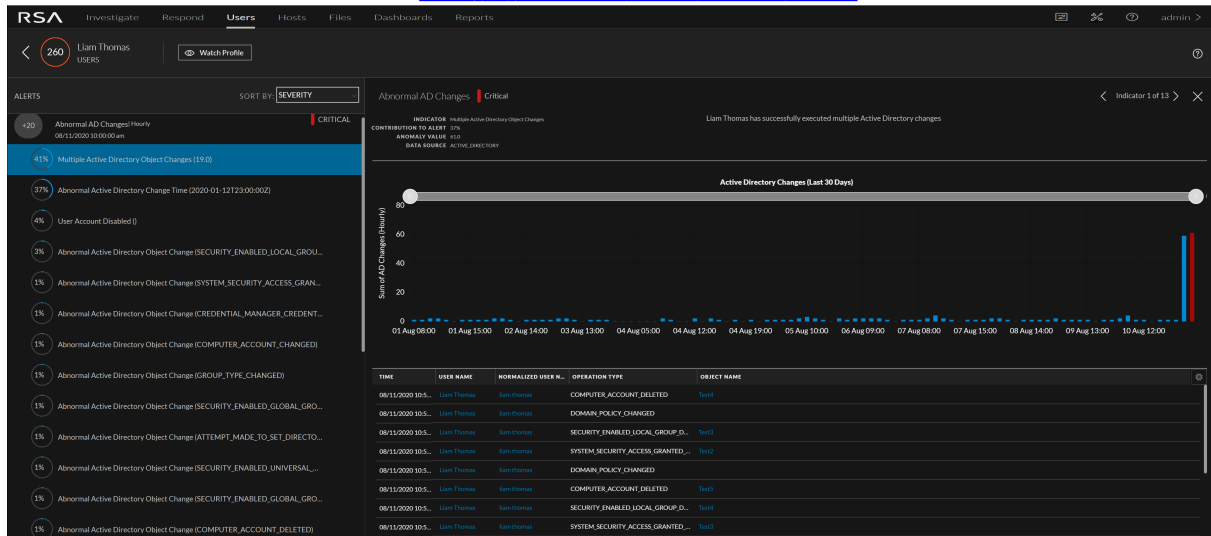
To pivot to the Events view:

1. Go to **Users** > **Alerts**, and select an alert or user or network entity.
   Indicators are displayed under the alert.

2. Select an indicator of interest.
   Values that can be used to pivot are highlighted in light blue at the bottom of the panel.
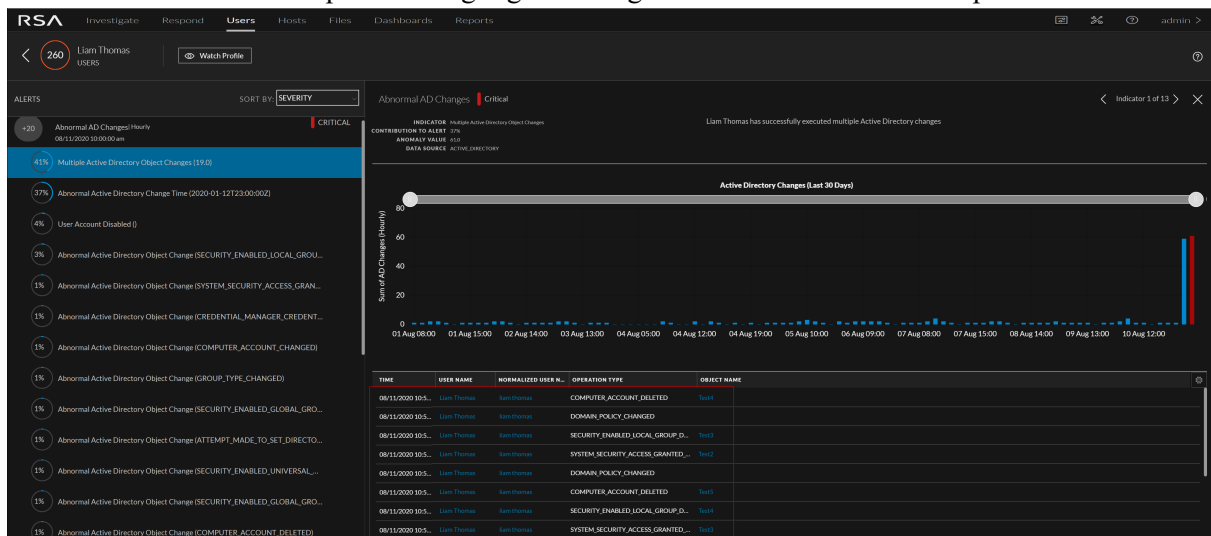
3. In the Events table, click the link highlighted in blue and pivot to the alert in the Events view.
   The Events view is displayed.
   For User events the username is a clickable pivot link. For JA3 and SSL Subject network entities events source IP, destination IP, destination country, destination organization, destination port, JA3 or SSL subject and source netname are the clickable pivot links.

For information about investigating items of interest in the Events view, see "Reconstructing and Analyzing Events" topic in the *NetWitness Investigate User Guide*.

To pivot to the Hosts Details view:

If you have NetWitness Endpoint installed, you can pivot to Hosts Details view for detailed information of the host.

1. Go to **Users** > **Alerts**, and select an alert or user or network entity.
   Indicators are displayed under the alert.

2. Select an indicator of interest.
   Details about the indicator are displayed in the right panel.

3. In the events table, click the events related to the host.
   The Host Details view is displayed.

For information about investigating items of interest in the Hosts view, see "Investigating Hosts" topic in the *NetWitness Endpoint User Guide*.

To pivot to the Analyze Process view:

If you have NetWitness Endpoint installed, you can pivot to Analyze Process view for detailed information about the process.

1. Go to **Users** > **Alerts**, and select an alert or user or network entity.

2. Select an alert name. Indicators are displayed under the alert.

3. Select an indicator of interest.
   Details about the indicator are displayed in the right panel.

4. In the Events table, click the events related to the process.
   The Analyze process view is displayed.

For more information, see "Investigating a Process" topic in the *NetWitness Endpoint User Guide*.

For more information on how to read the indicator charts, see Reading an Indicator Chart topic.

Manage Top Alerts

You can export a list of all alerts to a .csv file format. You can use this information to compare the data from other sources in other data analysis tools like tableau, powerbi, and zeppelin.

To export alert data to a .csv file:

1. Go to **Investigate** > **Entities** > **Alerts**.
   The Alerts tab is displayed.

2. On the top right, click **Export**.

All the alert data is downloaded in a .csv file format. The following figure is an example of the exported alert data in .csv format:

Set Alert Feedback Status

The analyst can mark alerts as **Not a Risk** or they can remove the **Not a Risk** feedback status by updating it to **None**. Also, multiple alerts grouped by date can be selected to perform this action.

To set an alert feedback status:

1. Go to **Users** > **Alerts**.

The Alerts tab is displayed with a list of alerts.

2. Select the checkbox and click Not a Risk to mark all the alerts as not risky.
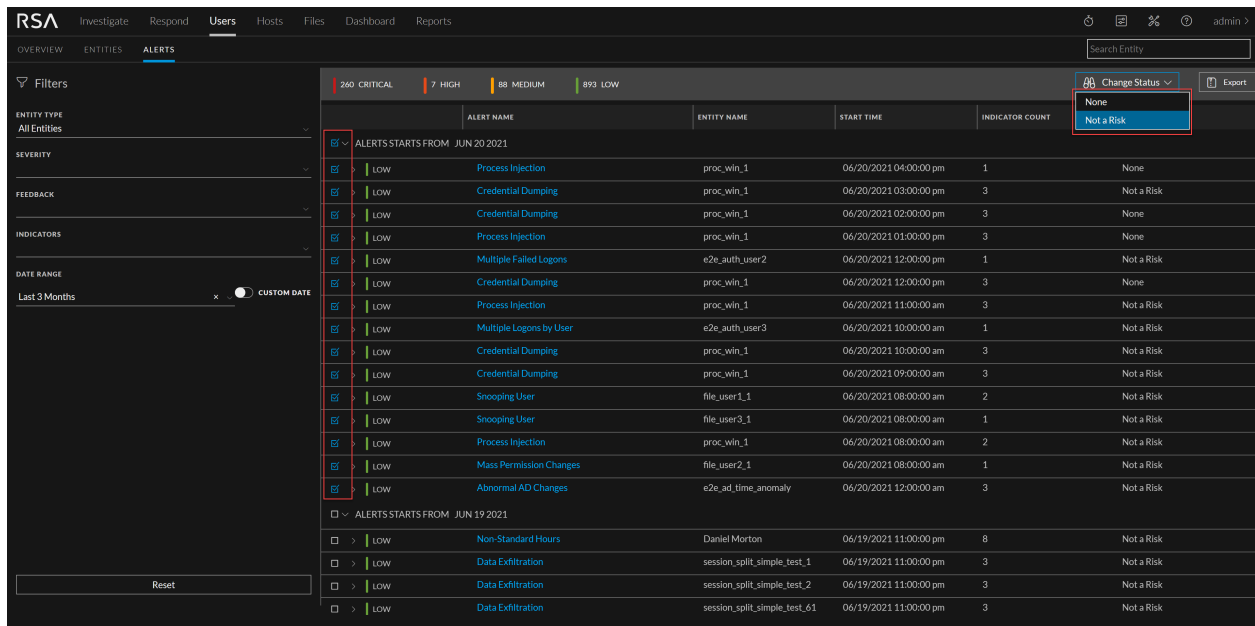
A confirmation message is displayed to confirm the change.

3. Click **OK**, to confirm the status or click **Cancel** if you don't want to continue with the update.

> **Note:** All alerts that are marked as Not a Risk will not contribute to the entity's score.

View Modeled Behaviors

(From 11.5.1 and later) NetWitness UEBA Modeled Behavior provides analysts with visibility into all the activities of a user. These modeled behaviors are based on the log data leveraged by UEBA and are available a day after the UEBA service is configured and running. UEBA monitors abnormal user behaviors to identify risky users and this requires data to be processed for a certain period of time. However, modeled behaviors reflect all the activities of the user within a day of the service configuration.

For example, if a user fails multiple times by logging in with incorrect credentials within an hour, analysts can view these behaviors as **Failed Authentications** for the user.

> **Note:**
> - Modeled Behaviors are not applicable to network entities.
> - By default, the sorting and data source options are disabled when there is no data available.

To view the Modeled Behaviors:

1. Log into NetWitness Platform and click **Users**.

2. Do one of the following:

   - In the **Overview** tab, under **Top Risky Users** panel, click on a username.

   - In the **Entities** tab, click on a username.

3. Click the **Modeled Behaviors** tab, to view the Modeled Behaviors highlighted with a blue line in the left panel. The results can be sorted by the date or in alphabetical order.
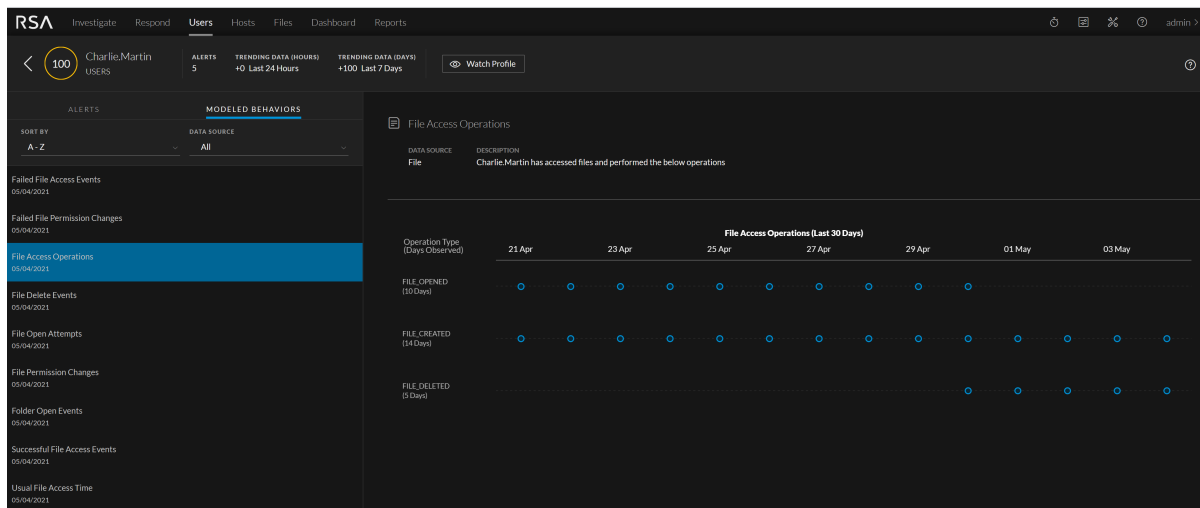
4. Select the data source from the drop-down according to your preference and filter the modeled behaviors:

   - Active Directory

   - File

   - Authentication

5. Based on the data source you select, the following information is displayed on the right panel:

- Data source name

- Modeled Behavior description

- A graph is displayed that contain details of a specific Modeled Behavior. You can view the modeled behaviors of a user for the last 30 days. The type of graph can vary, depending on the type of analysis performed by UEBA. The following figure is an example of a Modeled Behavior.
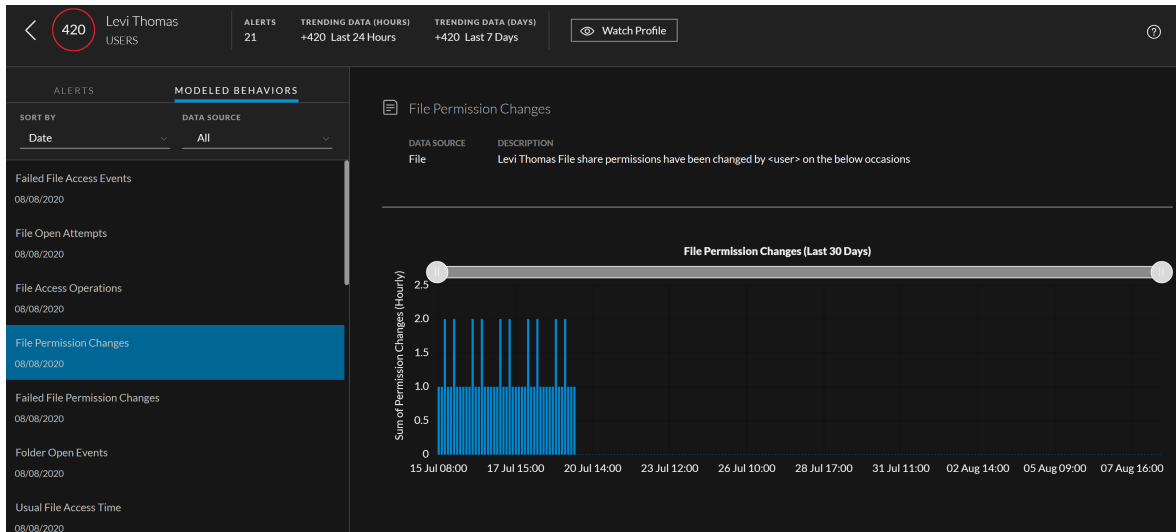
Reading an Indicator Chart

> **Note:** In version 11.6 and later, the pie chart was replaced by the dotted chart.

An indicator chart is a pictorial illustration of the anomaly and baseline values of an entity that you want to further investigate.

The chart gives the Analyst a better insight of the indicator which in turn will help determine the next steps. The chart provides the analyst with the user's baseline values over time to better understand the context of the anomaly.

To view an indicator chart,

1. Log in to NetWitness Platform.

2. Navigate to **Users** > **Entities**.

3. Select the user you want to investigate.
   The following figure displays an alert for a user logged on to an abnormal host.
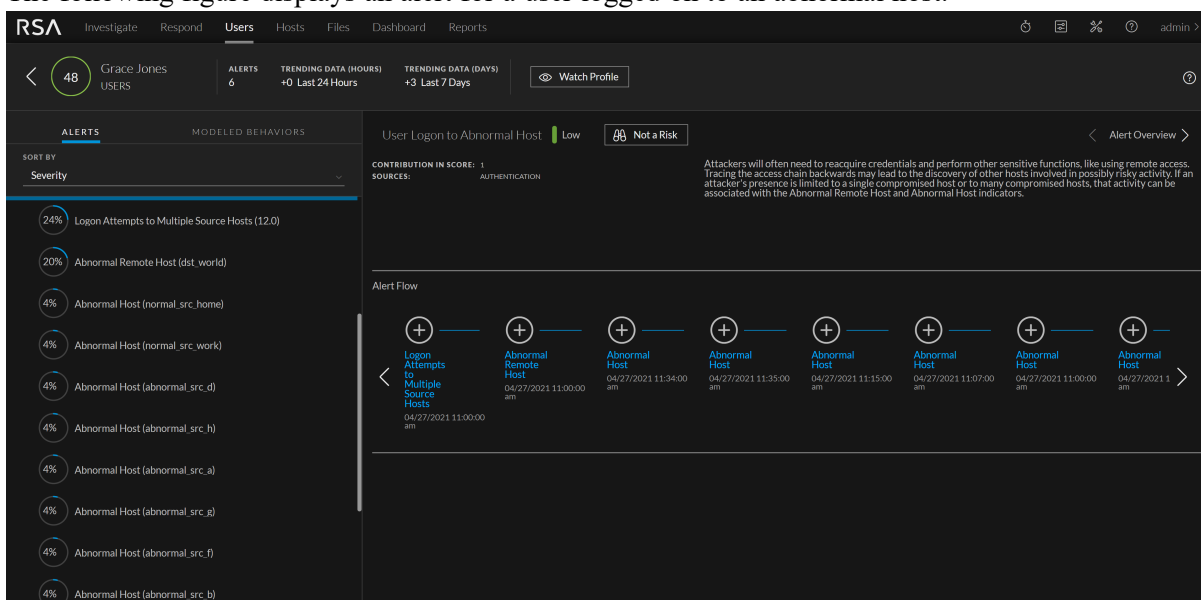
4. In the Alert Flow section, select the Logon Attempts to Multiple Source Hosts.

5. Click the + icon to expand and view the details.
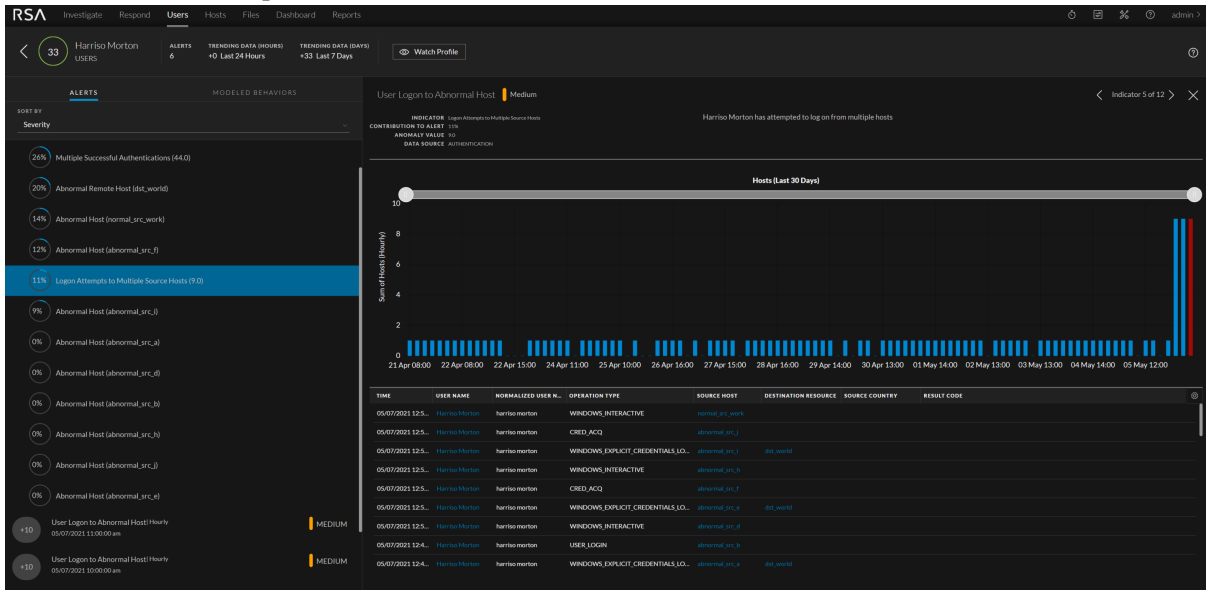
Types of Charts

There are three main types of charts currently available.

Continuous Bar Chart

In this type of an indicator chart, the bar color differentiates the behavior by displaying a blue bar and a red bar. For example, the following figure displays in a span of 30-days the number of Active Directory changes made on a daily basis which are displayed by blue bars and indicates the baseline behavior.

The red bar indicates that the user has accessed a high number of files in a specific hour.
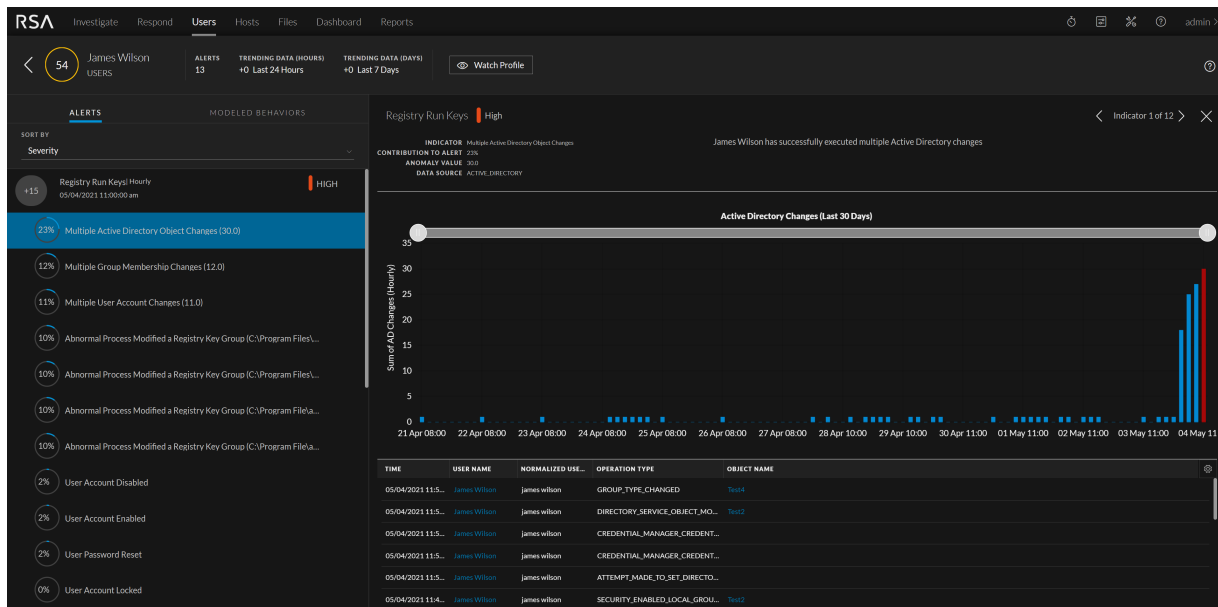
Another variation in the visualization of the chart is where you see an additional series of grey bars that represents the baseline values of the model. In this case, if the blue bars series is displayed, it depicts the specific entity trend that the anomaly is also a part of.

Dotted Chart

In the dotted indicator chart, the anomaly is displayed on top of the graph indicated by yellow color text and red color circle. The chart provides the analyst with the user's baseline values over time to better understand the context of the anomaly. The additional values (apart from the anomaly value) depicted in the Y-axis, represent the baseline values and the total number of days they were observed for this specific entity.
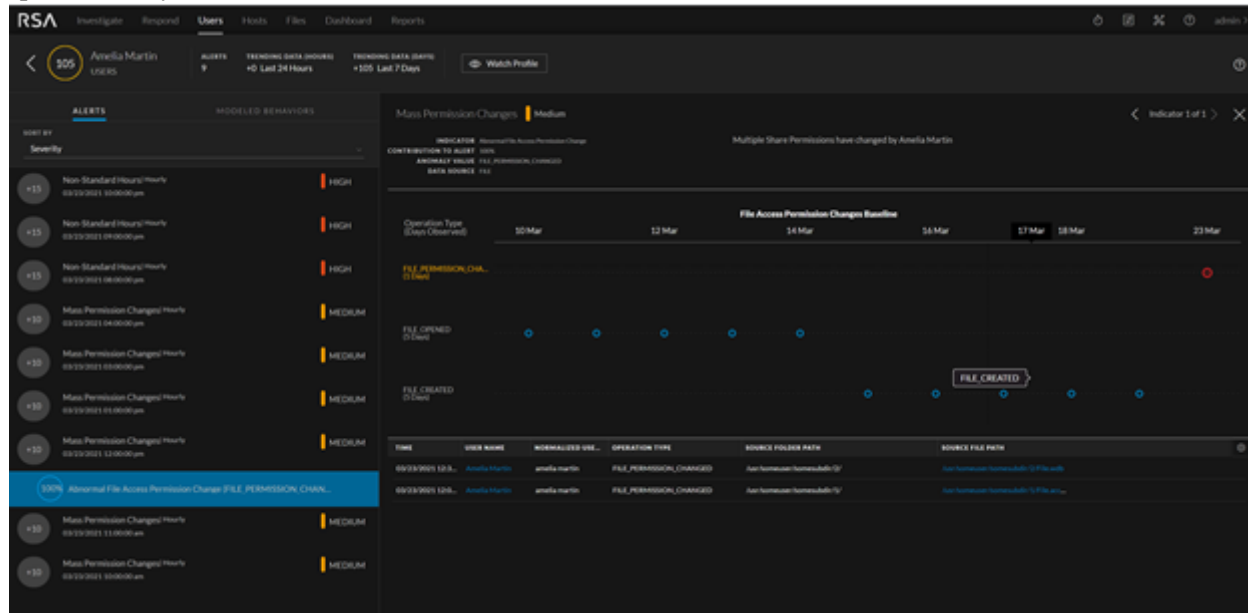
Time Chart

The time indicator chart displays the time the user has accessed a particular information. For example, in the following figure, the user has accessed Active Directory at an abnormal time over the past 30 days. The regular working hours of the user are the baseline values and the anomaly value (the hour marked in red) indicates that this is an abnormal time for this user to make changes in AD.
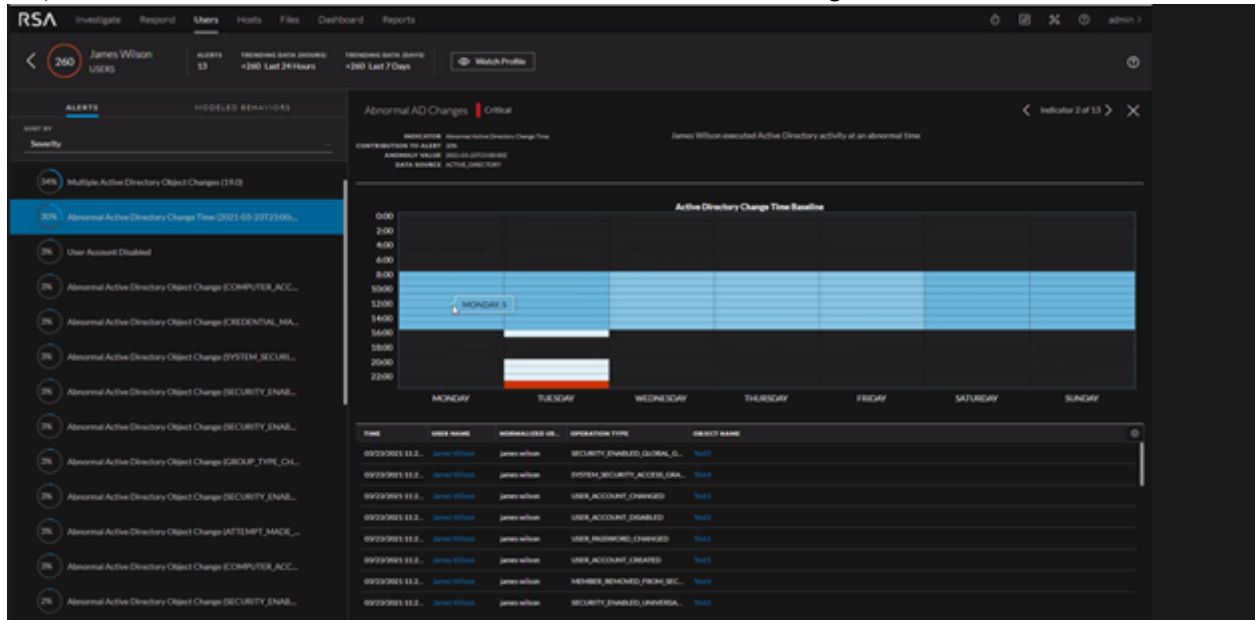
View NetWitness UEBA Metrics in Health and Wellness

RSA NetWitness UEBA sends metrics to the System Stats Browser tab in ⚙ **(Admin)** > **Health and Wellness**. Along with basic system usage information, metrics that are specific to NetWitness UEBA users, alerts, and events are provided.

Analysts can use these metrics in the following ways:

- Confirm that the currently procured license is in compliance with their license agreements, and by how much per day.

- Determine if the system is functioning as required.

- Actively monitor new events.

- Monitor the creation of new indicators and alerts.

If these critical metrics are reported as "0", it may indicate a system malfunction.

To view NetWitness UEBA metrics in the System Stats Browser in Health and Wellness:

1. Go to ⚙ **(Admin)** > **Health & Wellness**.

2. Click the **System Stats Browser** tab.
   The System Stats Browser is displayed.

3. Under Host, select **UEBA**, and then click **Apply**.
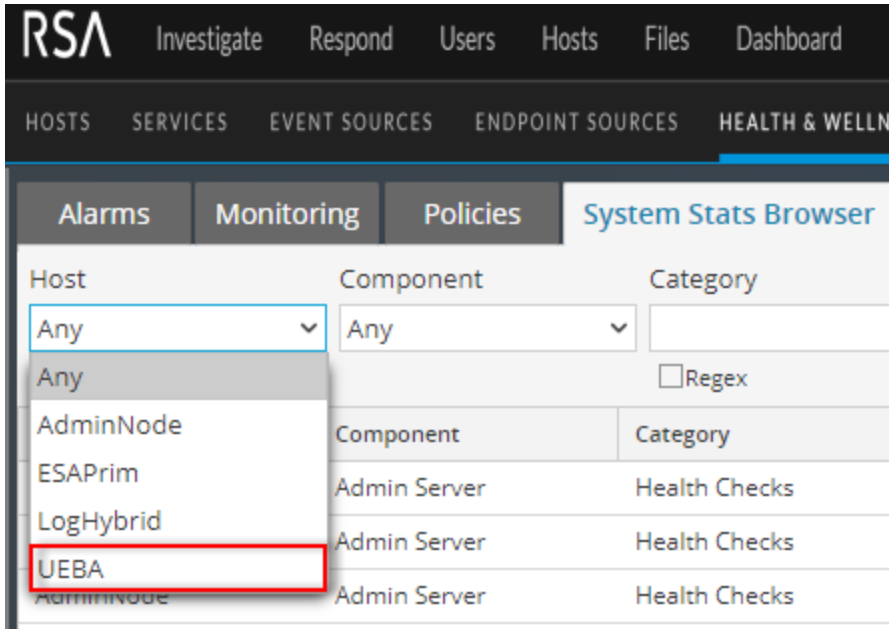
Results for NetWitness UEBA are displayed.

4. To view details for a statistic, click **Stat Details**.

The details of the statistics are displayed.

The **Name** and **Description** fields provide a summary of the metrics that are displayed.

For more information about Health and Wellness and System Stats Browser tab, see "Monitor System Statistics" topic in the *System Maintenance Guide*.

Monitor Health and Wellness of UEBA

You can view the status of UEBA host in the **Users** > **OVERVIEW** tab.

The UEBA system should generate at least one alert weekly. If the system stops generating the alerts for a period of seven days or more, advanced monitoring is required to monitor statistics about the total number of events versus successful events, total number of alerts generated, and so on.

Advanced monitoring is enabled through a third-party tools prepackaged in NetWitness: Kibana and Airflow.

Access Kibana

To access kibana, go to `https://<UEBA_host>/kibana/app/kibana#/,` enter user name and password and the Dashboard is displayed.
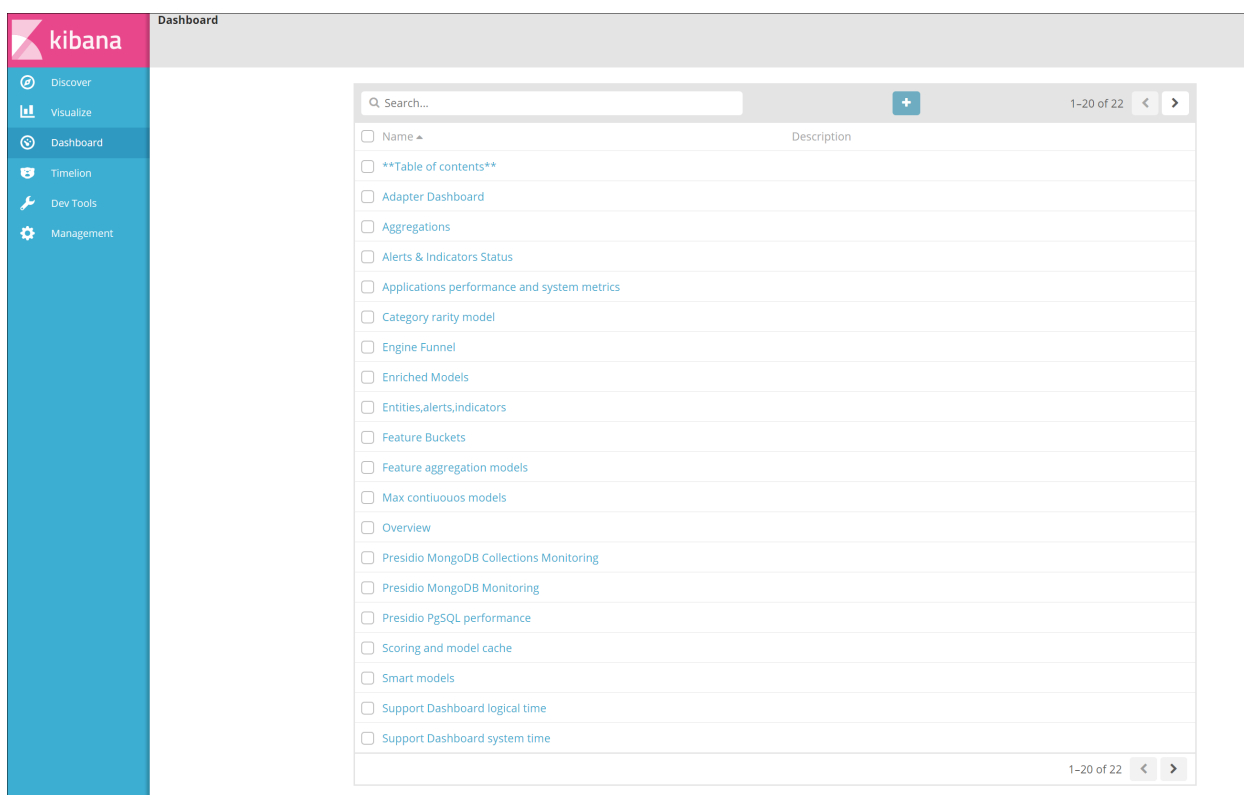
Access Airflow

To access Airflow, go to `https://<UEBA_host>/admin/,` enter user name and password and the DAGs view is displayed.

> **Note:** The Kibana and Airflow web server user interface password is the same as the deploy_admin password. Make sure that you record this password and store it in a safe location.

Kibana

Kibana is an open source analytics and visualization platform. You can monitor the health of UEBA through various dashboards:

Overview Dashboard

The Overview dashboard provides the statistics over the analytics about the users, entities, alerts, and indicators, such as:

- The alerts type that are generated, and the alert severity distribution with the severity types (Low, Medium, High, Critical).

- Total number of active entities and how many alerts are generated for those entities.

- The number of indicators and events processed.

- The pie chart for entity score severity and distribution for the alerts classification.

- Alert daily histogram, which is the total number of alert per each severity triggered over time.

To access the overview dashboard:

1. Go to Kibana, click **Dashboards** > **Overview**.
   The Overview dashboard is displayed with the aggregate results for all entities.
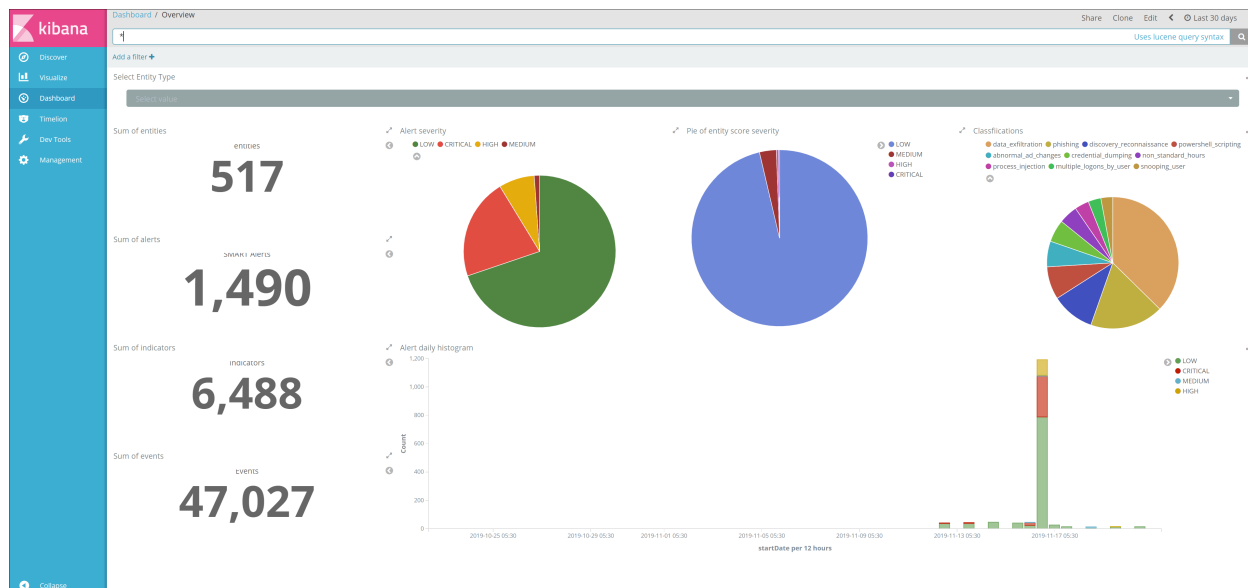
2. To view the data for a specific entity, select a value from the **Select Entity Type** drop-down. For example, ja3, sslSubject, or userid.

3. Adjust the time range on the top-right corner of the page based on your requirement to view the statistics.
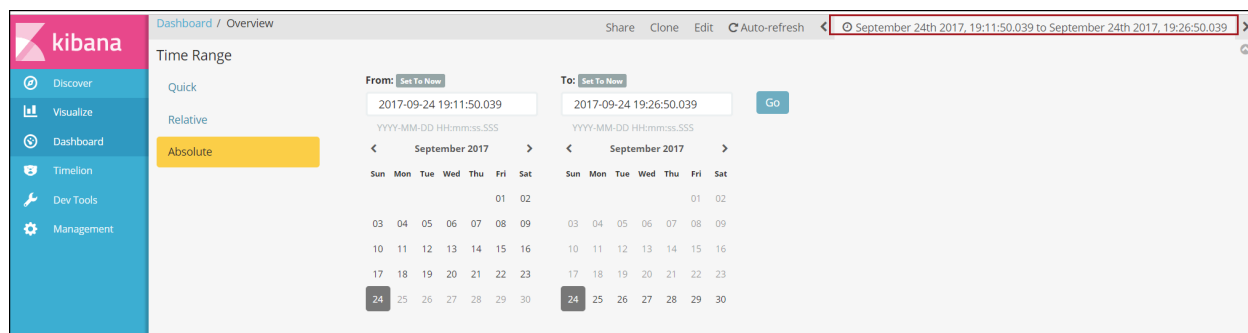
System Host overview

The System Host overview dashboard monitors the performance and health of UEBA hosts, such as:

- CPU usage.

- Memory consumption, and network.

- Process consuming CPU and Memory, for example MongoDB.

- Statistics over the disk usage.

- Inbound data is the amount of data transferred by user to view the UEBA UI.

- Outbound data is the amount of data fetched by UEBA from Broker or Concentrator.

To access System Host overview dashboard

1. Go to Kibana, click **Dashboards** > **System host overview**.
   The System host overview dashboard is displayed.
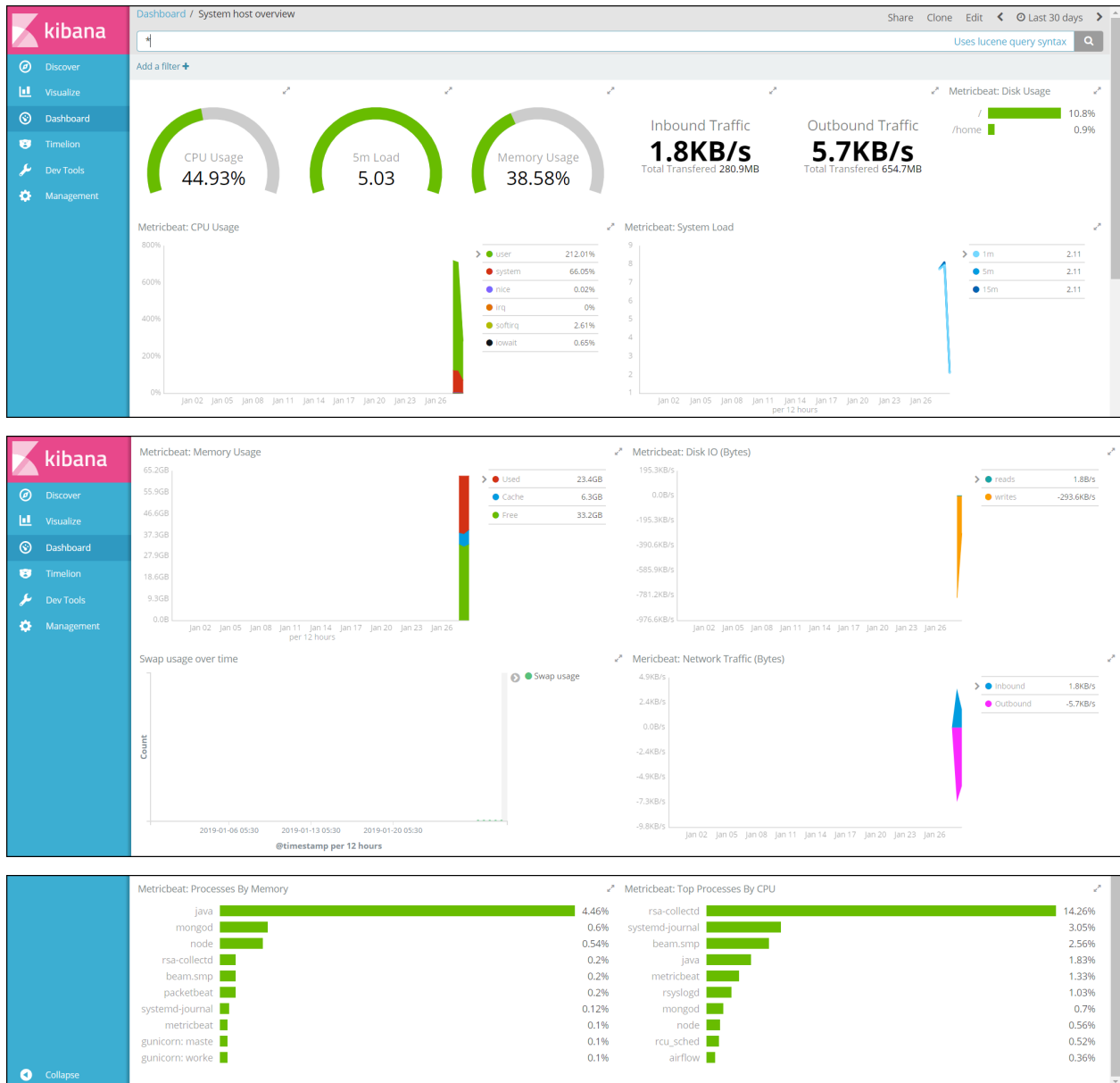
2. Adjust the time range on the top-right corner of the page based on your requirement to view the statistics.

> **Note:** During historical load, the system works in high parallelism. Due to that IO, CPU, and Memory is in high utilization. The pace would be 30 logical days four wall clock time. Once the UEBA server is online, the resource utilization reduces.

Adapter Dashboard

The **Adapter** dashboard is used to monitor the following:

- The failed events distribution.

- Total number of events versus successful events.

- Saved events per schema.

To access the entities, alerts and indicators

1. Go to Kibana, click **Dashboards** > **Entities, alerts, indicators**.
   The Entities, alerts, indicators Dashboard is displayed with an aggregate data for all entities.
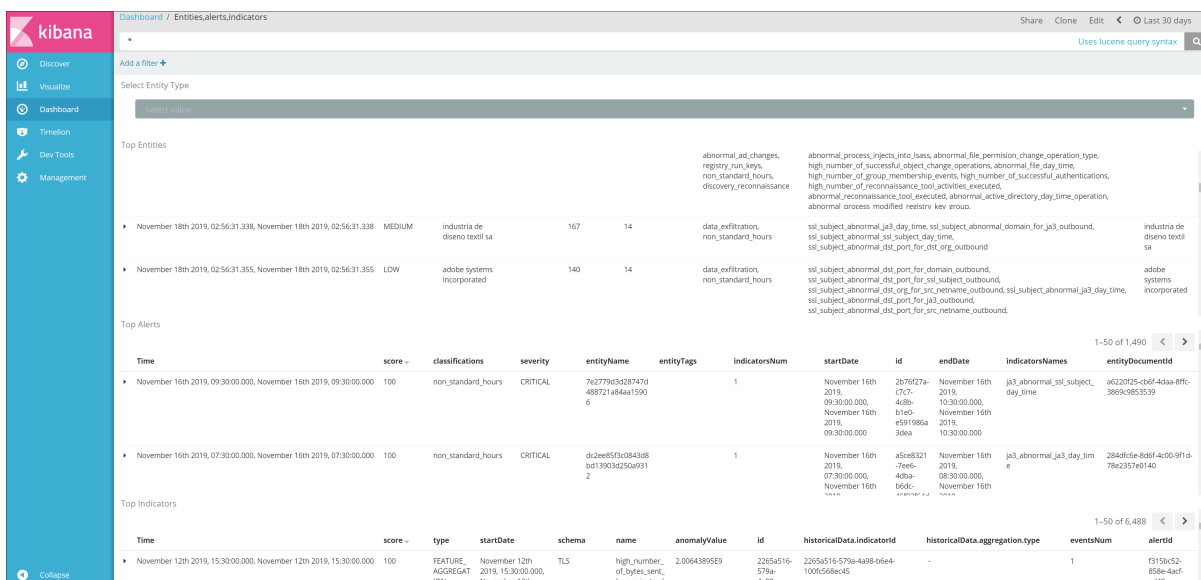
2. To view the data for a specific entity, select a value from the **Select Entity Type** drop-down. For example, ja3, sslSubject, or userid.

To access the adapter dashboard system Time

1. Go to Kibana, click **Dashboards** > **Adapter**.
   The Adapter Dashboard is displayed.
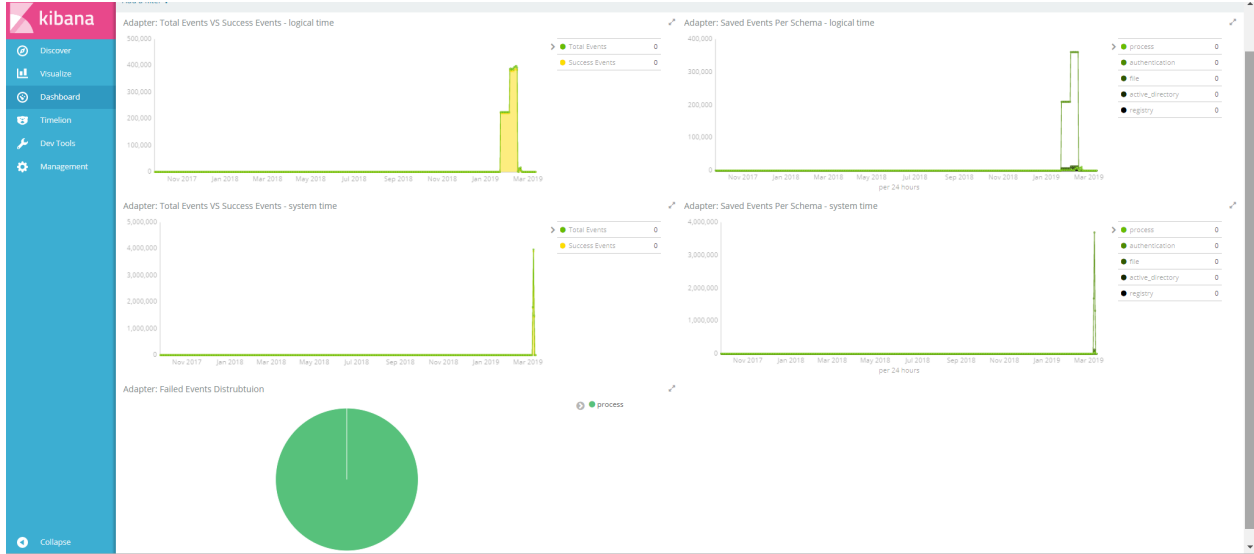
2. Adjust the time range on the top-right corner of the page based on your requirement to view the statistics.

Support Dashboard Logical Time

The **Support Dashboard Logical Time** provides the capability to detect events processed time, which is different from the system time, such as:

- The amount of filtered events over time per schema

- The total number of alerts generated

- The alert types distribution

- The events that are related to an alert

To access support dashboard logical time:

1. Go to Kibana, click **Dashboards** > **Support Dashboard Logical Time**.
   The Support Dashboard logical time is displayed.

2. Adjust the time range on the top-right corner of the page based on your requirement to view the statistics.
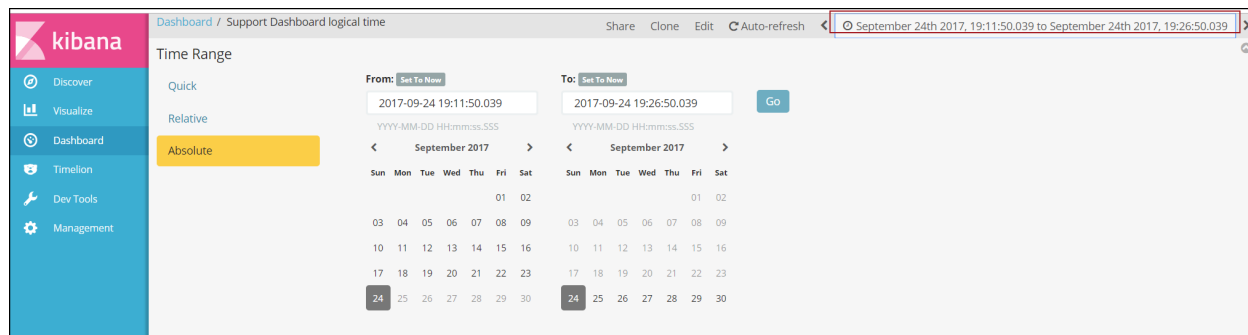
Support Dashboard System Time

The support dashboard system time allows you to monitor the system time when events are processed.

*   The amount of filtered events over time per schema.

*   The total number of alerts generated.

*   The alert types distribution.

*   The events that are related to an alert.

To access support dashboard system Time:

1. Go to Kibana, click **Dashboards** > **Support Dashboard system Time**.
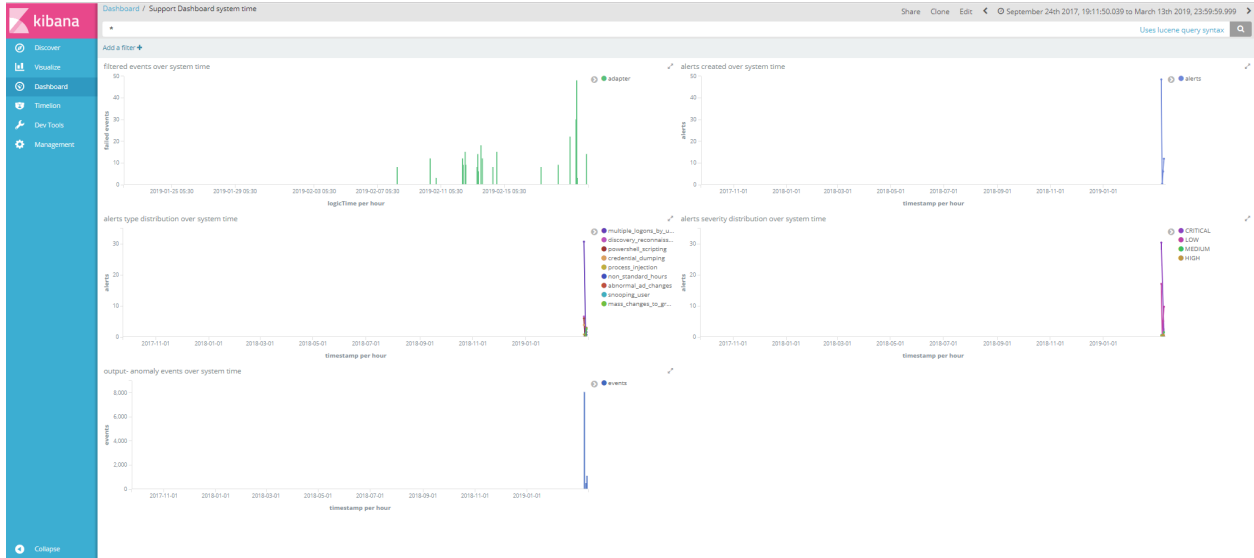
2. Adjust the time range on the top-right corner of the page to view the statistics.
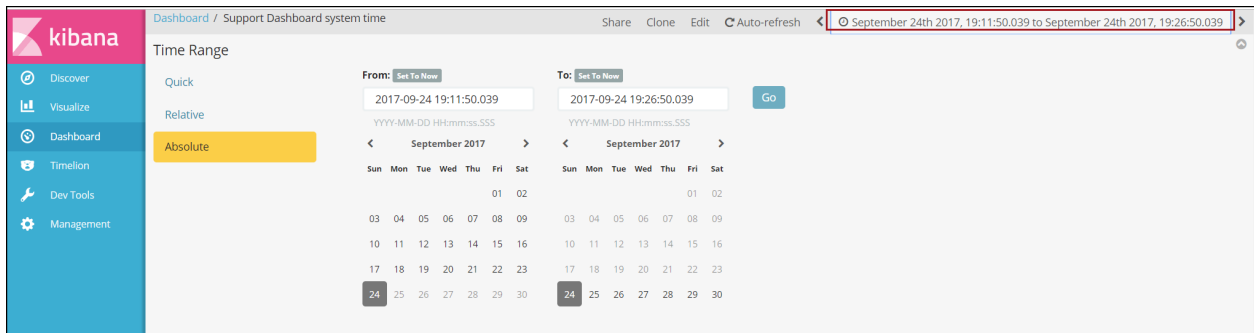
Scoring and Model Cache

The Scoring and Model cache dashboard provides the capability to view events being scored.

To access scoring and model cache dashboard:

1. Go to Kibana, click **Dashboards** > **Scoring and Model Cache**.
   The Scoring and model cache dashboard is displayed.
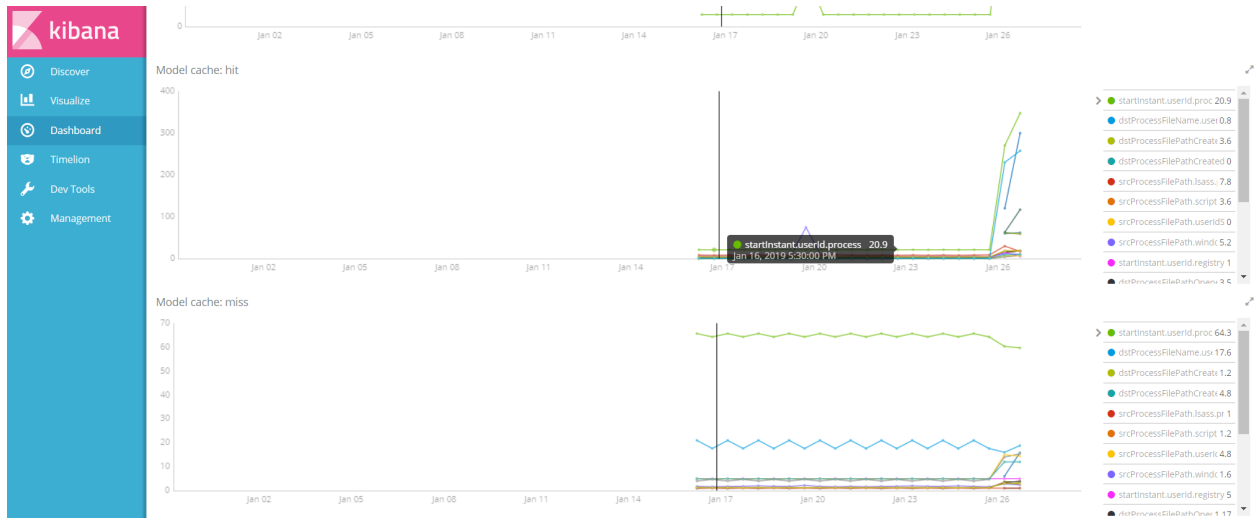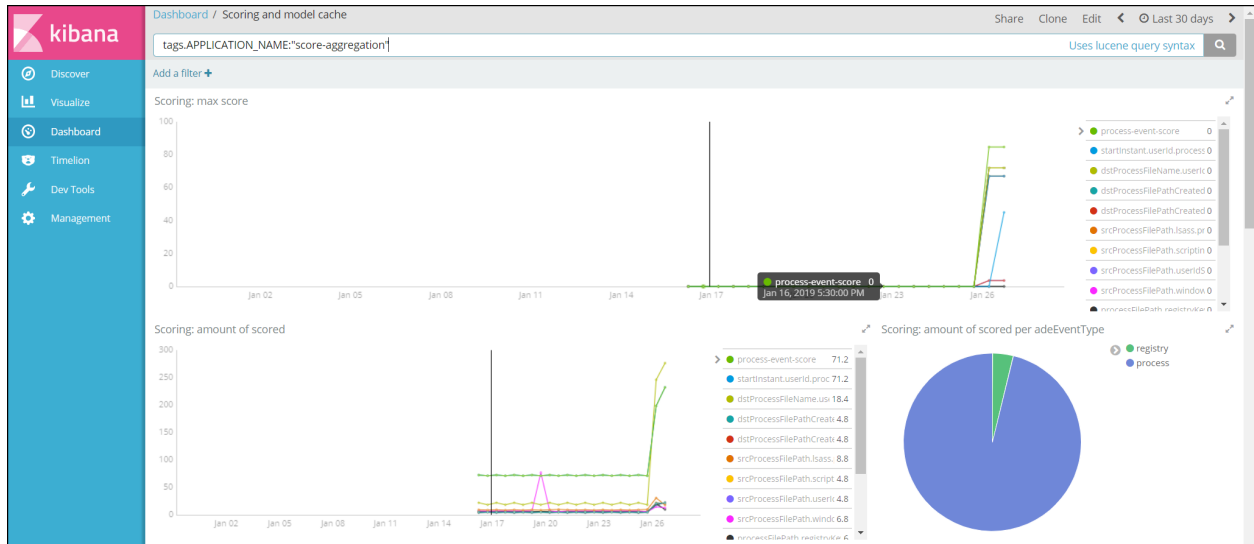
2. Adjust the time range on the top-right corner of the page to view the statistics.

Airflow

Airflow is a tool for describing, executing, and monitoring the UEBA tasks. In Airflow, a DAG is a collection of all tasks you want to run, organized based on the schemas that reflects their relationships and dependencies. For example, schemas such as Active Directory, Authentication, File, Process, TLS and Registry. Each schema is divided into two:

•   Indicator DAG which is responsible to read events from broker and score the events based on the models.

•   Model DAG which is responsible in building the models.

You can monitor the scheduled task by seeing how many tasks are successful, failed, or currently running.

There are several DAGs and each DAG is a workflow.

To monitor UEBA service tasks, perform the following:

1. Go to **Airflow**.
    The DAGs view is displayed.

2. In the **DAG Runs** section, see the status of the tasks. For example, how many tasks are successful, failed or currently running.

3. To view the different tasks associated with the DAG, click **Tree view**.
The Tree view of the DAG is displayed.
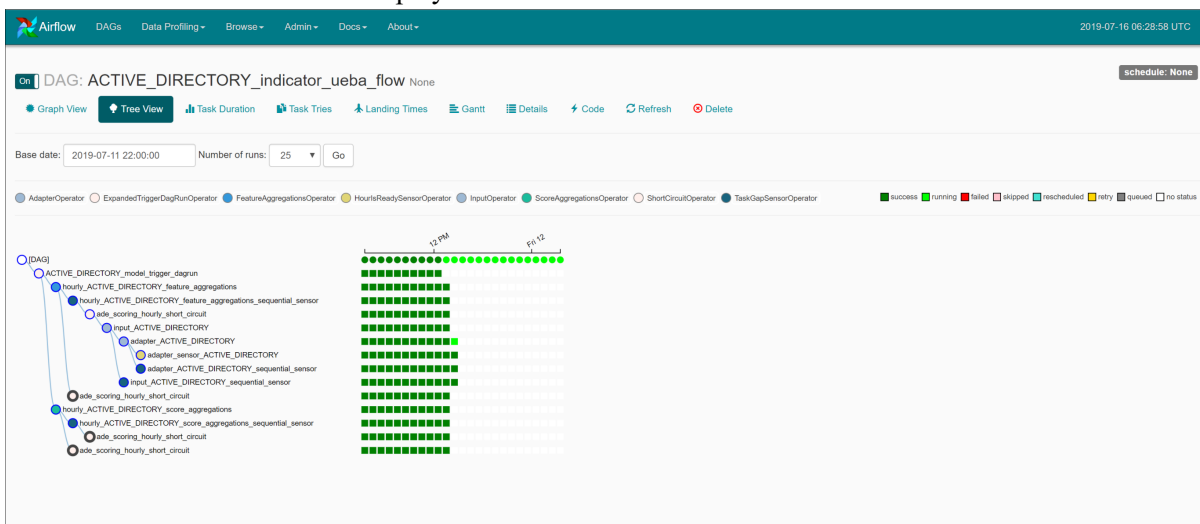
4. To view the DAG's dependencies and the current status of a specific task, in the DAG, click **Graph view**.
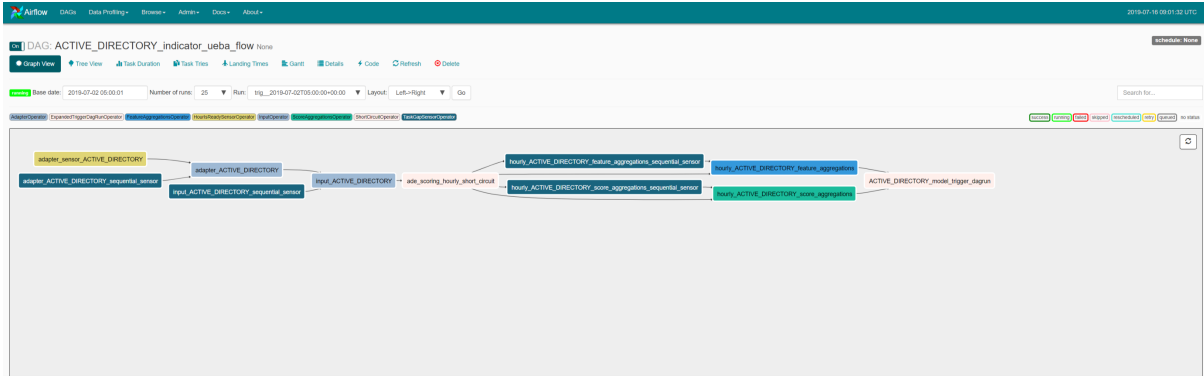
In the **Graph** view, hover over the task to see the status of the specific task.
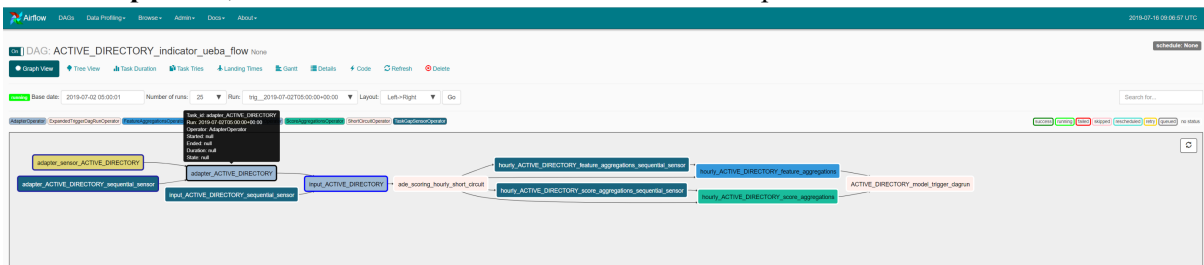
For detailed information about the specific task, click **Task** and click **Task Instance Details.**

The Task Instance Details view is displayed.

To view the logs of the specific task, click **Log**.

Note: After you begin to run a DAG, schemas cannot be removed from UEBA, otherwise the process will stop. For more information see, 'Troubleshooting UEBA Configurations' topic in the *UEBA Configuration Guide.*.

Reference

This section provides information about the RSA NetWitness UEBA user interface.

Overview Tab

The Overview tab provides an initial view into the recent and most important user or network entity activities in the environment. Each panel shows either prioritized incidents for investigation or consolidated metrics reflecting potential risks to the enterprise.

Workflow
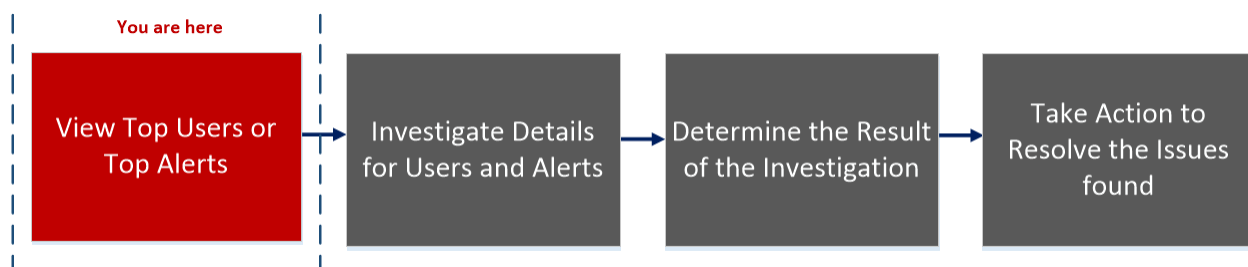
What do you want to do?

User Role	I want to ...	Documentation
UEBA Analyst	View top ten high-risk users or network entities.*	Identify High-Risk User or Network Entity
UEBA Analyst	View risky user or network entities, and watchlist or network entities.*	Identify High-Risk User or Network Entity
UEBA Analyst	View user based on alert type and indicator.	Identify High-Risk User or Network Entity
UEBA Analyst	Investigate alerts in my environment.	Investigate Top Alerts
UEBA Analyst	Begin an investigation of critical alerts.	Investigate Top Alerts
UEBA Analyst	Sort alerts to focus my investigation.	Filter Alerts
UEBA Analyst	Investigate threat indicators.	Investigate Events
UEBA Analyst	Export alert data.	Manage Top Alerts

*You can complete the tasks here.

Related Topics

- [Begin an Investigation of High-Risk User Or Network Entity](#)

- [Investigate Top Alerts](#)

- [Filter Alerts](#)

- [Manage Top Alerts](#)

Quick Look

The following figure shows the Overview tab.
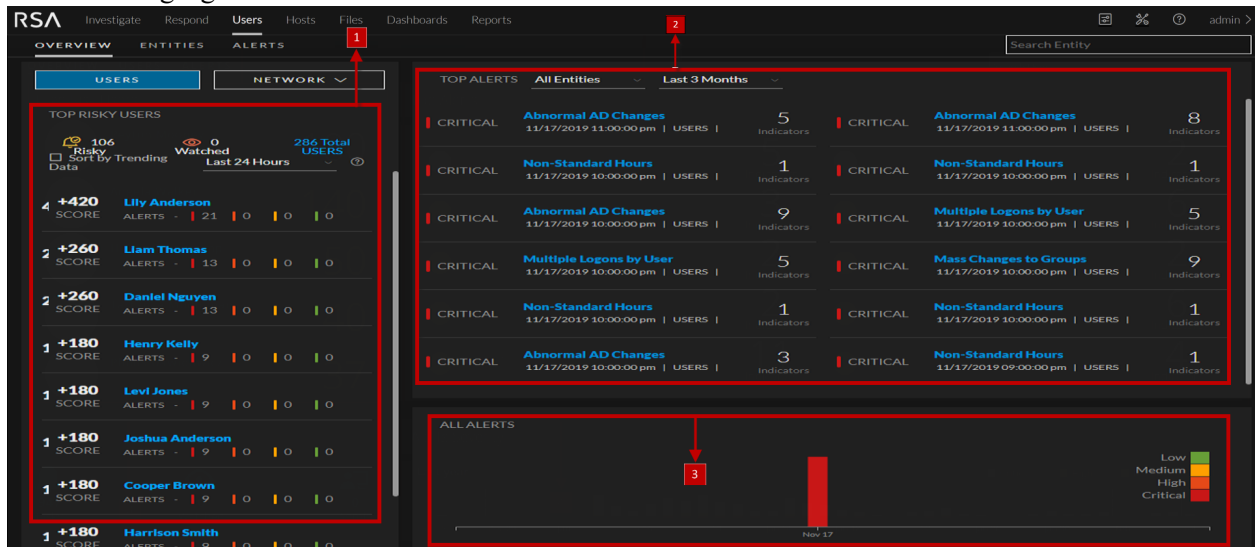
The Overview tab consists of the following panels:

1   Top Risky User or Network entities panel
2   Top Alerts panel
3   Alerts Severity panel

Top Risky User or Network Entity Panel

The High Risk User or Network entities panel lists the top ten high-risk users or network entities along with the user or network entity score.

In this example, the following table describes the high risk users panel elements.

Name	Description
Risky	All user or network entities with a risk score greater than 0.
Watched	All user or network entities who are currently flagged as Watched.
Total Users	All user or network entities in the network.

Name	Description
User or Network entity name	The name of the user or network entity.
User or Network Entity Score	The score of the user or network entity, with the color indicating the severity of the score. • red indicates critical • orange represents a high risk • yellow indicates a medium risk • green represents a low risk

Top Alerts Panel

The Top Alerts panel displays a list of alerts for the associated user or network entity, severity, alert creation date, and number of indicators. The list consists of the top ten alerts in the Last 24 Hours, Last 7 days, Last 1 Month and Last 3 Months.

The following table describes the top alerts panel elements.

Name	Description
Severity Icon	The alert severity icon. The options are Critical, High, Medium, or Low.
Alert Name	The name of the alert.
Alert Creation Date	The date when an alert is generated.
Number of Indicators	The number of indicators associated with the alert.

Alerts Severity Panel

The Alert Severity panel graphically displays the number of alerts.

The following table describes alert severity panel elements.

Name	Description
Severity level	The severity is color coded, where red indicates a Critical alert, orange represents a High risk alert, yellow indicates a Medium risk alert, and green represents a Low risk alert. For example: ■ Critical ■ High ■ Medium ■ Low

Entities Tab

The Entities tab is a proactive threat hunting console. You can use behavioral filters to build use-case driven target lists, and to continuously monitor the environment for specific risky behavior patterns.

Workflow
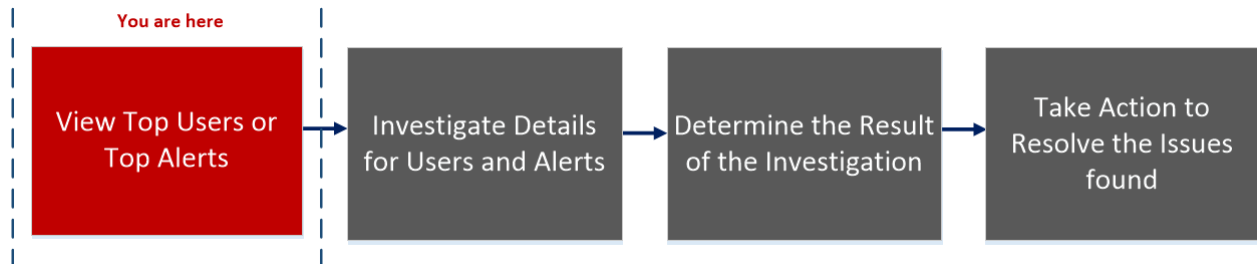
What do you want to do?

User Role	I want to ...	Documentation
UEBA Analyst	View high-risk users or network entities*.	Identify High-Risk User or Network Entity
UEBA Analyst	View user or network entity based on alert type and indicator*.	Identify High-Risk User or Network Entity
UEBA Analyst	Begin an investigation of high-risk user or network entities.	Begin an Investigation of High-Risk User Or Network Entity
UEBA Analyst	Take action on high-risk users or network entities*.	Take Action on High-Risk User or Network Entity
UEBA Analyst	Export high-risk users or network entities*.	Export a list of High-Risk User or Network Entity
UEBA Analyst	Begin an investigation of critical alerts.	Investigate Top Alerts
UEBA Analyst	Investigate threat indicators.	Investigate Events

*You can complete the tasks here.

Related Topics

- Begin an Investigation of High-Risk User Or Network Entity
- Investigate Top Alerts

- [Filter Alerts](#)

- [Investigate Events](#)

- [Export a list of High-Risk User or Network Entity](#)

Quick Look

The following figure shows the Entities tab.
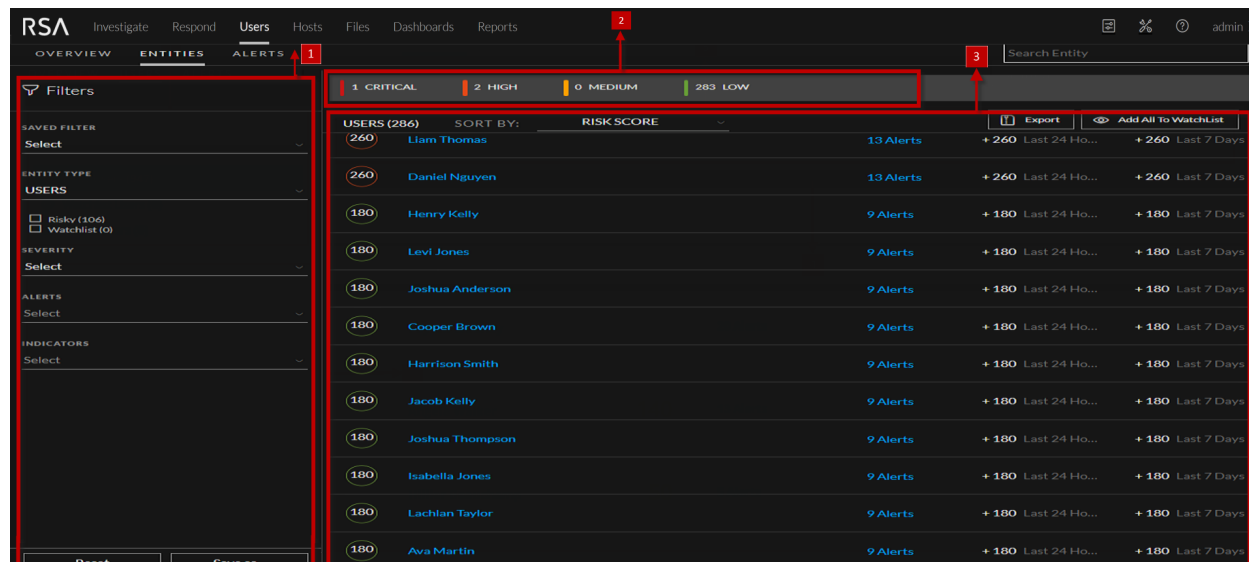
The Users tab consists of the following panels:

1	Filters panel
2	Risk Indicator Panel
3	User or Entity List panel

Filters Panel

The Filters panel lists two pre-defined filters, with the number of users associated with each in parentheses, and the list of behavioral profiles that are saved as favorites.

Filter Type	Description
Saved Filter	Previously saved behavioral filters.
Entity Type	Entity type such as Users, JA3, and SSL.
Risky User or Network Entities	All user or network entities with a risk score greater than 0.
Watchlist User or Network Entities	All user or network entities that are currently flagged as Watched.
Severity	Severity type, such as critical, high, medium and low.

Filter Type	Description
Alerts	Any of the existing alert types that describe the supported distinct use cases (Brute Force Attempt, Snooping User, Abnormal AD Change, Data Exfiltration).
Indicators	Any of the existing behavioral features modeled by NetWitness UEBA. This filter can also be used to target only alerts from a specific data source or application.
Reset	Reset the filter.
Save as	Save the filters as favorites.

Risk Indicator panel

The Risk indicator provides a severity-based breakdown of the target user or network entities.

The following table describes the risk indicator panel elements.

Color	Severity
Red	Critical
Orange	High
Yellow	Medium
Green	Low

Entities List Panel

The Entities List panel displays the list of all the user or network entities in your environment along with the user or network entity score and number of alerts associated with the user or network entity.

The following table describes the Entities List panel elements.

User Data	Description
Username or Network entity name	The name of the user or network entity.
Score	The user or the network entity.
Number of alerts	The total number of alerts generated for the user or network entity.
Sort by	The Sort by drop-down menu allows you to select the sorting method for the list. The options are: Risk Score, Name, Alerts, Trending last 24 hours, and Trending last 7 days.
Export	Export a list of all user or network entities and their scores in a .csv file format.
Add All to Watchlist	Adds all user or network entities in the filtered view to the watchlist.
Search Entity	Searches for a user name or a network entity that you typed, allows you to select it from the list that is displayed matching your entry.

Alerts Tab

The Alerts tab displays details about all alerts in your environment. You can view forensic information about suspicious activity in your environment that is based on a specific timeframe.

Workflow
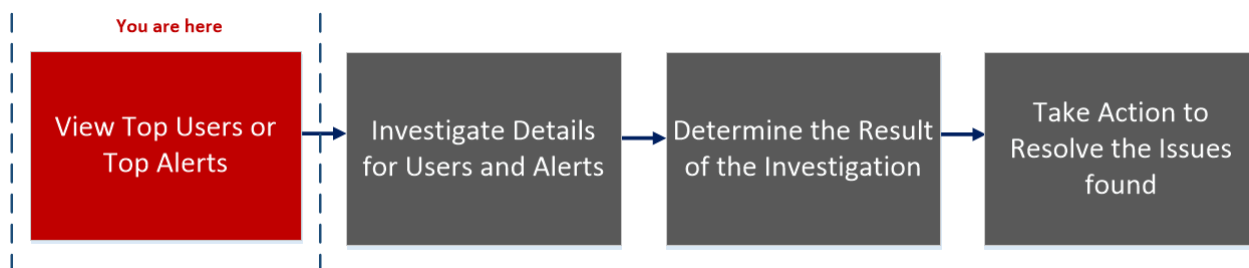
What do you want to do?

User Role	I want to ...	Documentation
UEBA Analyst	Investigate alerts in my environment*.	Investigate Top Alerts

User Role	I want to ...	Documentation
UEBA Analyst	Sort alerts to focus my investigation*.	Filter Alerts
UEBA Analyst	Investigate incidents based on threat indicators*.	Investigate Events
UEBA Analyst	Share alert data in spreadsheet format.	Manage Top Alerts

*You can complete the tasks here.

Related Topics

- Investigate Top Alerts

- Filter Alerts

- Investigate Events

- Manage Top Alerts

Quick Look
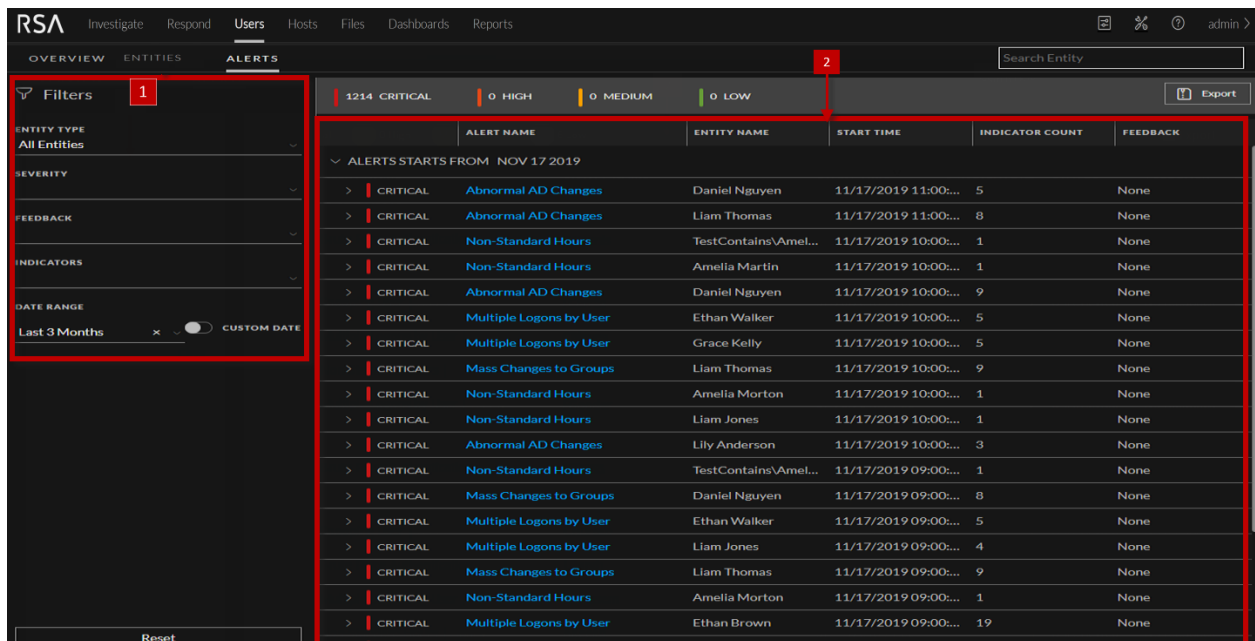
The Alerts tab consists of the following panels:

| 1 | Filters panel
| 2 | Alerts panel

Filters Panel

Use the filters panel to refine your investigation of alerts. The filters are automatically applied as you make your selections. You can reset all currently set filters by clicking **Reset**.

The following table describes the filters types.

Filter Name	Description	Options
Entity Type	Filters the list of alerts to include only alerts for a specific user name.	All Entities, Users, JA3, and SSL
Severity	Filters the list of alerts to include alerts for one or more severity levels.	Critical, High, Medium, or Low.
Feedback	Filters the list of alerts to include alerts for one or more feedback types.	Select All, No Feedback, or Not a Risk.
Indicators	Filters the list of alerts to include alerts for one or more indicators.	Examples of indicators are: • Active Directory - Abnormal Logon Time • Authentication - Logged onto Multiple Computers • Multiple File Access Failures
Date Range	Filters the list of alerts to include alerts created during a specific time range.	Last 7 days, Last 2 weeks, Last 1 month, Last 3 months, Last 6 month or specified range.

Alerts Panel

The Alerts panel displays the following information for each alert:

- Severity Icon: An icon next to the alert name that indicates the severity level of the alert.

- Alert Name: The name of the alert and the alert timeframe.

- Entity Name: The name of the entity that generated the alert.

- Start Time: The date and time when this alert was first detected.

- Indicator Count: The number of unique behavior anomalies (indicators) associated with the alert.

- Feedback: Indicates if a feedback value assigned for the alert.

At the beginning of each alert line is an arrow that expands the alert to display additional details. When you expand, the following fields are displayed:

- Indicator Name – The name of each unique indicator that is associated with the alert.

- Anomaly Value – The indicator's value, representing the deviation amount or value as it differs from the user's normal behavior.

- Data Source – The type of data where the indicator was found.

- Start Time – The date and time when this indicator was first detected.

The data that is currently displayed in the central pane can be exported to a .csv file by clicking **Export** at the top right of the pane.

User or Network Entity Profile View

The **User Network Entity Profile** view provides detailed information about all alerts and related indicators of a user or network entity.

Workflow

What do you want to do?

User Role	I want to ...	Documentation
UEBA Analyst	View high-risk user or network entities*	Identify High-Risk User or Network Entity
UEBA Analyst	Begin an investigation of high-risk user or network entities*	Begin an Investigation of High-Risk User Or Network Entity
UEBA Analyst	Take action on high-risk user or network entities.	Take Action on High-Risk User or Network Entity
UEBA Analyst	Export high-risk user or network entities.	Export a list of High-Risk User or Network Entity
UEBA Analyst	Begin an investigation of critical alerts*	Investigate Top Alerts

User Role	I want to ...	Documentation
UEBA Analyst	Investigate threat indicators.	[Investigate Events](#)
UEBA Analyst	View Modeled Behaviors for users **Note:** From 11.5.1 version and later, Modeled Behaviors for users can be viewed.	[View Modeled Behaviors](#)

*You can complete the tasks here.

Related Topics

- [Begin an Investigation of High-Risk User Or Network Entity](#)

- [Investigate Top Alerts](#)

- [Filter Alerts](#)

- [Investigate Events](#)

- [Export a list of High-Risk User or Network Entity](#)

- [View Modeled Behaviors](#)

Quick Look
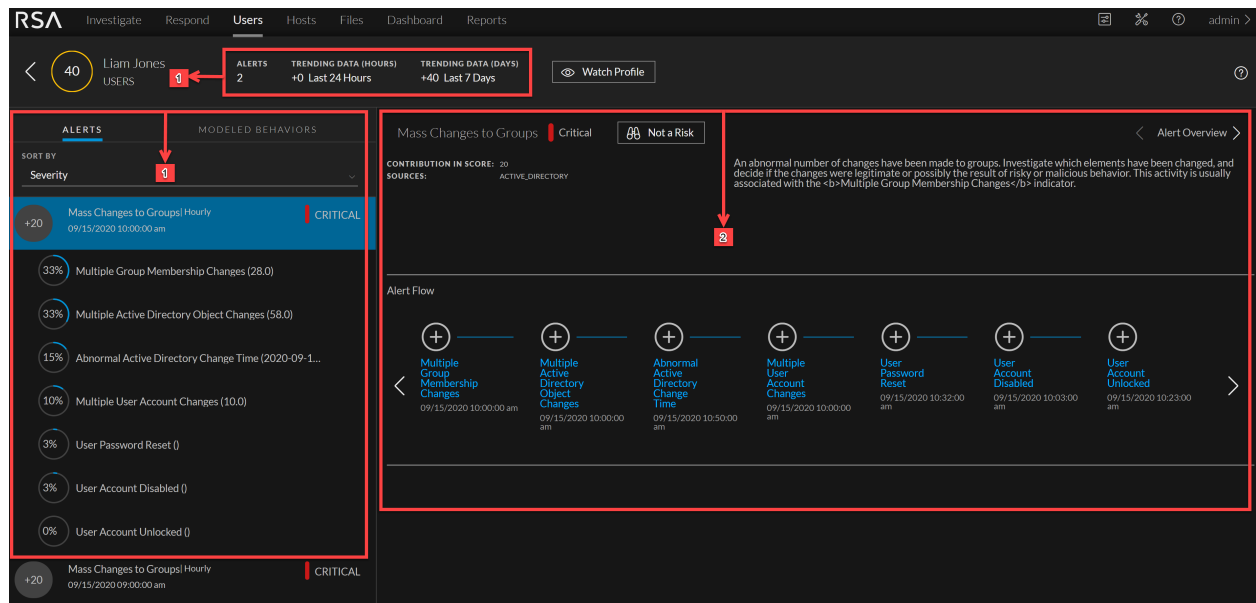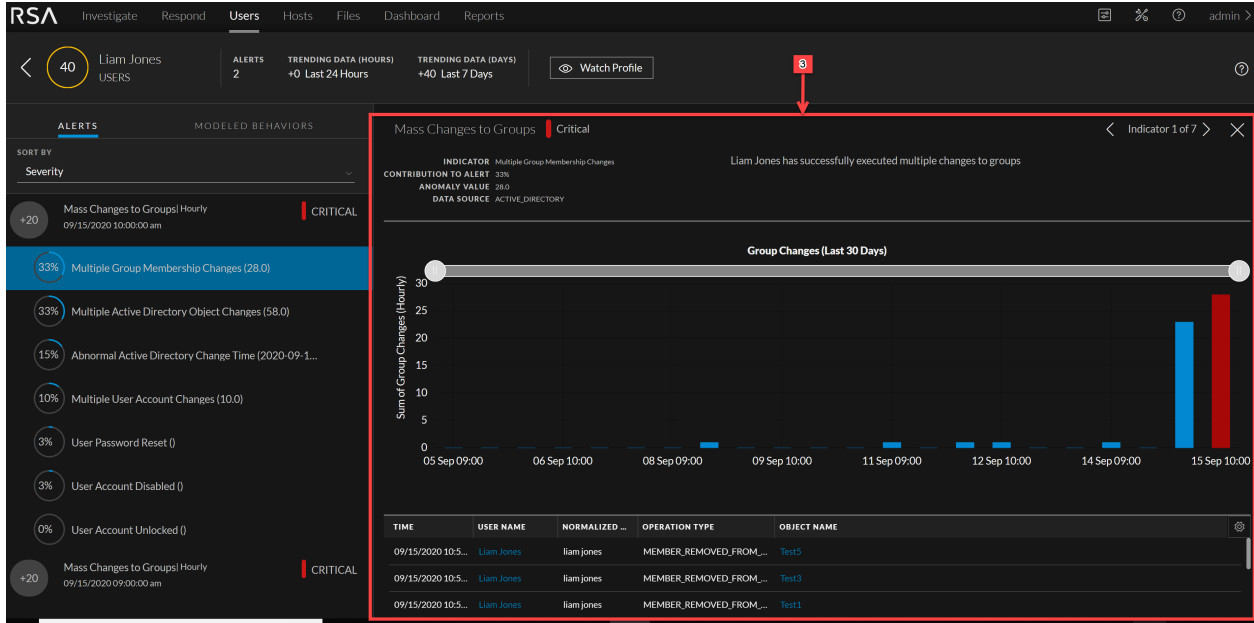
The following figure shows the User Modeled Behaviors view.
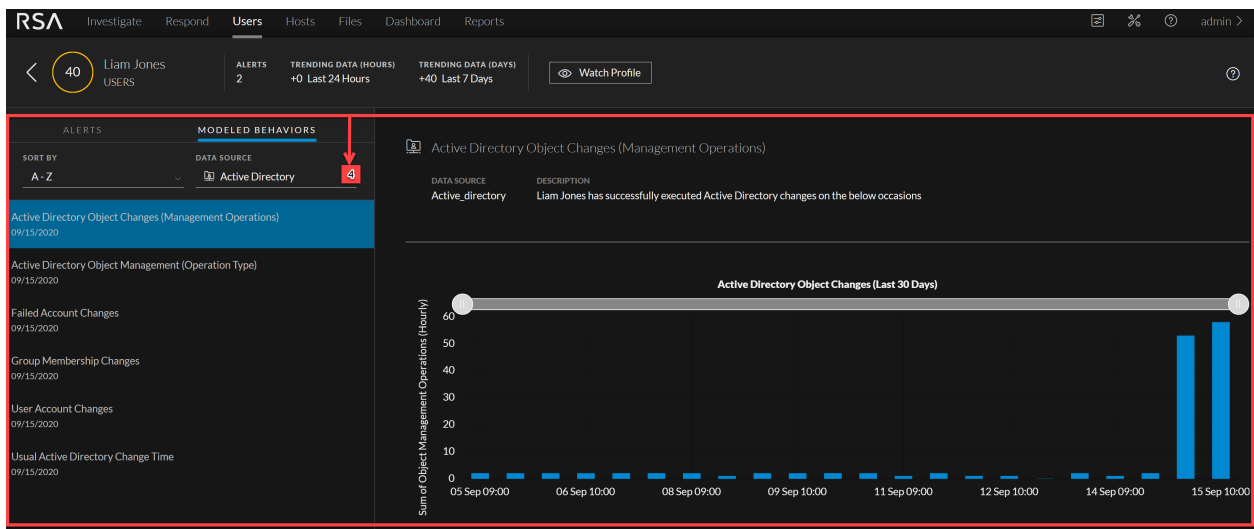
The Users Profile consist of the following panels:

1	User Risk Score panel
2	Alerts Flow panel
3	Indicator panel
4	Modeled Behaviors panel

User or Network Entity Risk Score Panel

The User or Network Entity Risk Score panel contains the following information:

Name	Description
User Score	The user score of the user highlighted based on the severity.
Alerts	The total number of alerts generated for the user in the last 90 days.
Trending Data (Hours)	The trending data for last 24 hours shows the increase in the user's score in the last 24 hours.
Trending Data (Days)	The trending data for last 7 days shows the increase in the user's score in the last 7 days.
Alerts	The following information is displayed: • alert names • severity level icon • start date and time for the alert • timeframe of the alert (Hourly) • risk score of the alert (+20) • list of alert indicator names and the number of times the indicator events occurred.
Sort by	The alerts are sorted based on Severity and Date. By default, it is sorted by severity.

Alert Flow Panel

The Alert Flow panel displays the following information:

Name	Description
Alert name	The name of the alert.
Time frame	The timeframe of the alert (hourly).
Severity level	The severity of the alert.
Contribution in score	The contribution to the user score value (for example, +20).
Sources	The data sources for the alert (for example, Active Directory).
Tamerlane graph	The timeline of events that are related to the formation of the alert.

Indicator Panel

Click on a graph icon in the Alert Flow panel to open the Indicator panel. The following table describes the indicator panel elements:

Name	Description
Indicator	The name of the indicator with timeframe of the indicator in parentheses. For example, Multiple Group Membership Changes (Hourly).
Contribution to Alert	The alert contribution percentage.
Anomaly Value	The anomaly value.
Data source	The data source from where the alert is triggered.

In the Indicator panel the events table list events specific to the data sources.

- **Common events for User Entity**

The following tables list events specific to all the data sources.

Event Name	Description
Time	The date and time when an event is triggered.
Username	The name of user for whom an indicator is triggered.
Normalized user name	The name of user for whom an indicator is triggered.
Operation Type	The action performed by the user. For example, Member Added To Group.

Event Name	Description
Result	The status of the action performed by the user.

- **Windows File Servers**

The following tables list events specific to Windows file servers.

Event Name	Description
Source Folder Path	Absolute folder path of a file for which an event is triggered.
Source File Path	Absolute file path for which an event is triggered.

- **Active Directory**

The following tables list event specific to Active Directory.

Event Name	Description
Object Name	Object name defined in the Active Directory.

- **Logon Activity**

The following tables list events specific to Logon Activity.

Event Name	Description
Computer	Host name from where an event is triggered.

- **Process**

The following tables list events specific to Process.

Event Name	Description
Machine Name	Name of the host from where this event is triggered for the user.
Source Process	Process triggered by the event
Destination Process	Process triggered by source process.

- **Registry**

The following tables list events specific to Registry.

Event Name	Description
Machine Name	Name of the host from where this event is triggered for the user.
Process Directory	Absolute directory path of the process for which an event is triggered.
Process File Name	Process file name for which an event is triggered.
Registry Key Group	Type of registry key.
Registry Key	Registry key path.
Registry Value Name	Registry value name that is created or modified.
Operation Type	The action performed by the user. For example, Member Added To Group.

Network Entities

The following tables list events specific to JA3 and SSL Subject.

Event Name	Description
Source IP	The IP address from which network data is sent.
Destination IP	The IP address to which network data is sent.
Destination Country	The country name to which the network data is sent.
SSL	The SSL Subject.
Destination Organization	The organization name where the network data is sent.
Domain	The domain name to which the network data is sent.
JA3	The JA3 hash value.
Destination Port	The port number to which the network data is sent.
Source Netname	The name of the source netname.
Number of Bytes Sent	The number of bytes sent.
Destination ASN	
JA3S	The JA3S hash value.

Event Name	Description
Destination Netname	The name of the destination netname.
Number of Bytes Received	The number of bytes received.

Modeled Behaviors Panel

The Modeled Behaviors panel displays the following information:

Name	Description
Modeled Behaviors	The following information is displayed: • The data source names • The date of the user's last activity • Description of the Modeled Behaviors.
Data Source	The data source can be selected from the drop-down.
Sort by	The Modeled Behaviors are sorted based on date and alphabetical order. By default, it is sorted by alphabetical order.

Appendix: NetWitness UEBA Windows Audit Policy

To achieve maximum benefit from RSA NetWitness UEBA, RSA recommends that you implement the Windows audit policies described here.

For a base set of policies to audit, see the "Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008 Audit Settings Recommendations" section of this article from Microsoft: Audit Policy Recommendations.

The policies under "Stronger Recommendation" are required, and the following policies, to ensure that all of the required Authentication and Active Directory events are audited:

- Audit Detailed File Share

- Audit File Share

- Audit File System

RSA recommends that you enable auditing for both success and failures.

The following Windows events must be audited:

For the Authentication models:

4624	4625	4769	4628

For the AD models:

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					

For File Access Models:

4660	4663	4670	5145