RSA NETWITNESS® PLATFORM

NetWitness UEBA User Guide

for RSA NetWitness® Platform 11.4

Contact Information

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

Trademarks

For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks.

License Agreement

Third-Party Licenses

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

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

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

May 2020

Contents

Introduction

RSA NetWitness UEBA (User and Entity Behavior Analytics) 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 in your environment.

Users

All users in your organization can be analyzed using the log and endpoint data for abnormal user activities. The log and endpoint data is retrieved and parsed from the NetWitness Platform Database (NWDB).

Network

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

UEBA can be used 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 NetWitness Platform Database (NWDB) into the new TLS data source that supports two new entities namely JA3 and SSL Subject. These entities are used to 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 that is equipped to identify the client application initiating the session. The JA3 fingerprints are used to 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, hence the entity for which the certificate was issued.

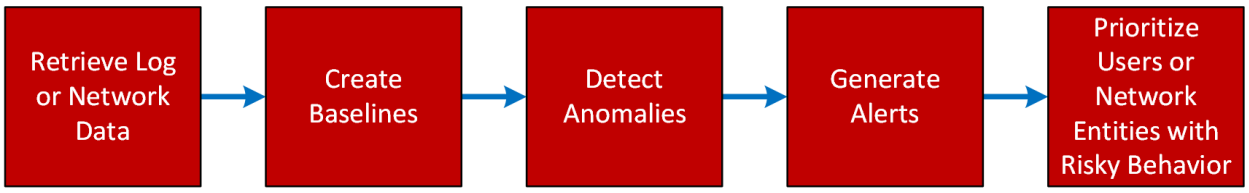
NetWitness UEBA enables analyst to:

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

This guide provides information and instructions for using all 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.

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. There are five basic steps to this process, as displayed in the following diagram:



The following table provides a brief description of each of these steps.

Step	Description	More Information
1. Retrieve Log and Endpoint or Network Data	NetWitness UEBA retrieves logs or endpoint or network data from the NetWitness Platform Database (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 from a user or network entity's 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 will be transformed into an alert.	See Generate Indicators and Generate Alerts

Step	Description	More Information
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 associated with them, or have 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 11.3 Physical Host Installation Guide*

Note: In 11.4, 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 Troubleshooting UEBA.

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 was abnormal for an user entity, but is not abnormal for the organization, the false-positive reduction algorithms decreases 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 the entities in your network. However, RSA recommends that you configure NetWitness UEBA to start baselining your data two months prior to your deployment date `<today-60days>`. The first 28 days will be used for model training and will not be 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, will be normalized, and then combined into one modeled entity. As a result, different users, who share the same username in different domains, will wrongfully 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. An example of 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 normal amount of data sent from an application or specific port that is contacted for 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 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 which is different from what is normal, it is a strong deviation. This abnormal behavior of communicating to an abnormal port or domain 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 either represent anomalies found in 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, 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 the 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 will be transformed into an alert, and the anomalies into indicators. A high-scored batch of anomalies becomes an alert that contains validated 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 could 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 behavior occurs, an alert is triggered.

Users

- Authentication from an abnormal computer
- Multiple authentication attempts identified in a short time frame
- Multiple files have been 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 beginning to generate new alerts. If historical audit data is processed when NetWitness UEBA is enabled, alerts appear after the historical data has been 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

Network Sources

- TLS in Version 11.4

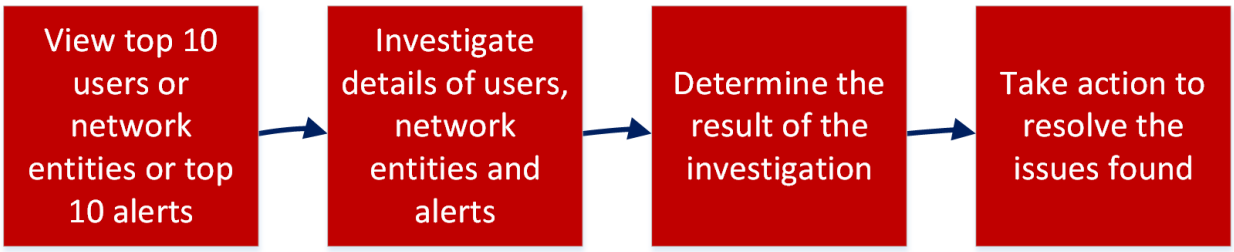
Recommended Workflows

To use NetWitness UEBA more effectively, there are two workflows; Detection workflow and Forensic workflow, that you can follow.

Detection Workflow

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

The following flowchart illustrates the steps you can follow to begin detecting suspicious behavior in your environment.



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 riskiest 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 into detailed information about risky user or entity behaviors and critical alerts to try 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 user interface from the previous steps and identify areas to focus on to resolve the issues you found.	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 the results of this investigation to improve and sharpen future investigations.	Take Action on High-Risk User or Network Entity

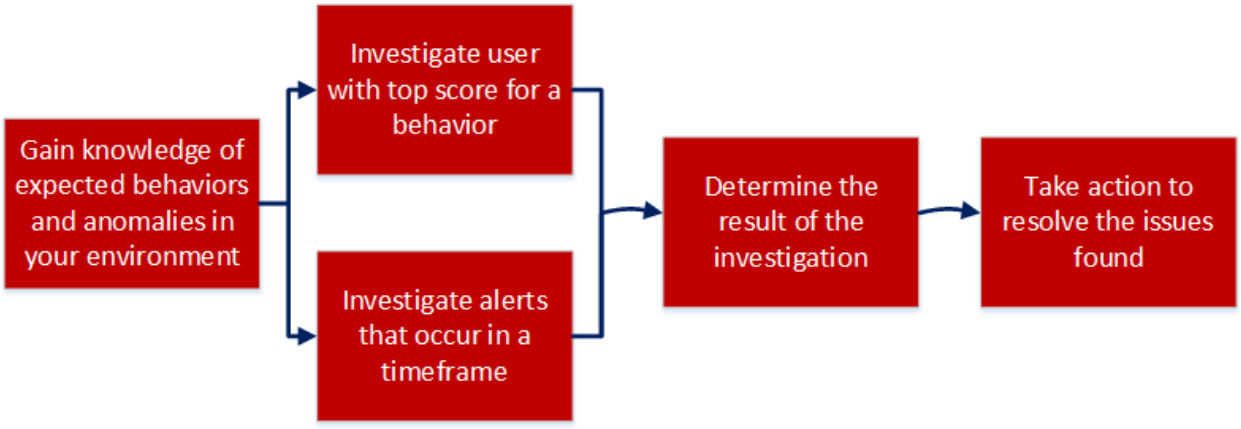
Forensic Workflow

The forensic workflow is recommended when you have gained 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 timeframe in which suspicious events occurred.

Using forensics information, analysts may determine the 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 your investigation on forensic information that is based on a specific user or entity behavior, or a specific timeframe 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, so that you can focus on anomalies that are significant for your environment.	Retrieve Data, Detect Anomalies, and Generate Alerts.
Investigate an 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 timeframe	Determine a timeframe of interest, and in the Alerts tab, select that timeframe to see detailed information about alerts that occurred during that time 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 User or Network Entity
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, malicious external attacker 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. 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 User .

Use Case for Network Entities

UEBA can detect malicious traffic masked within an 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 Entity.

Alert Types

Alert Types for User

Alert Type	Description
Mass Changes to Groups	An abnormal number of changes have been made to groups. Investigate which elements have been changed, and decide if the changes were legitimate or possibly the result of risky or malicious behavior. This activity is usually associated with the **Multiple Group Membership Changes** indicator.
Elevated Privileges Granted	Elevated account privileges have been delegated to a user. Attackers often use regular user accounts, granting them elevated privileges, to exploit the network. Investigate the user that received the elevated privileges, and decide if these changes were legitimate or possibly the result of risky or malicious behavior. This activity is usually associated with the **Nested Member Added to Critical Enterprise Group** and **Member Added to Critical Enterprise Group** indicators.
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 Logins to Multiple AD Sites	Domain controllers store credential password hashes for all accounts on the domain, so they are high-value targets for attackers. Domain controllers that are not stringently updated and secured are susceptible to attack and compromise, which could leave the domain vulnerable. User privileges on multiple domains could indicate that a parent domain has been compromised. Determine if user access to and from multiple sites is legitimate or is an indication of a potential compromise. This activity is usually associated with the **Logged into Multiple Domains** 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 Computer** indicator.

Alert Type	Description
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 ransomware, 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 has been infected with ransomware. This activity can be associated with the **Multiple File Rename Events** indicator.
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 another's 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 being 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 keychain 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 Computers** indicator.
Admin Password Change	Shared long-term secrets, for example, privileged account passwords, are frequently used to access anything from print servers to domain controllers. To contain attackers that seek to leverage these accounts, pay close attention to password changes by admins, and ensure they have been made by trusted parties and have no additional abnormal behavior associated with them. This activity can be associated with the **Admin Password Change** indicator.

Alert Type	Description
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 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.
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 has been 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.

Alert Type	Description
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 has been taken over by an external actor. This activity can be associated with the **Abnormal File Access 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, normally 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.
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.
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.
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.

Alert Types for Network Entity

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**, **Abnormal Domain for JA3**, **Abnormal Destination Port for JA3** 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 Destination Port for Source Netname** and **Abnormal Traffic Volume Sent from JA3** indicators.

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 changed multiple file share permissions.
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.

Indicator	Alert Type	Description
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	Description	Alert Type
Abnormal Active Directory Change Time	A user made Active Directory changes at an abnormal time.	Non-Standard Hours
Abnormal Active Directory Object Change	An abnormal change made to an Active Directory attribute.	Abnormal AD Changes
Multiple Group Membership Changes	A user successfully made multiple changes to groups.	Mass Changes to Groups
Multiple Active Directory Object Changes	A user made multiple Active Directory changes successfully.	Abnormal AD Changes
Multiple User Account Changes	A user successfully made multiple sensitive Active Directory changes.	Abnormal AD Changes
Multiple Failed Account Changes	A user failed to make multiple Active Directory changes.	Abnormal AD Changes
Admin Password Changed	An admin's password was changed.	Admin Password Change
User Account Enabled	A user's account was enabled.	Sensitive User Status Changes
User Account Disabled	A user's account was disabled.	Sensitive User Status Changes
User Account Unlocked	A user's account was unlocked.	Sensitive User Status Changes
User Account Type Changed	A user's type was changed.	Sensitive User Status Changes
User Account Locked	A user's account was locked.	Sensitive User Status Changes

Indicator	Description	Alert Type
User Password Reset	A user's password was reset.	Sensitive User Status Changes
User Password Never Expires Option Changed	A user has changed the password policy.	Sensitive User Status Changes

Logon Activity

Indicator	Alert Type	Description
Abnormal Remote Computer	Abnormal Computer Access	A user has accessed an abnormal remote computer.
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 an abnormal computer.
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 & Reconnaissance	An abnormal process is executed.
Abnormal Process Executed a Scripting Tool	PowerShell & Scripting	An abnormal process executed a scripting tool.
Abnormal Process Executed a Scripting Tool	PowerShell & Scripting	An abnormal process is triggered by a scripting tool.
Scripting Tool Triggered an Abnormal Application	PowerShell & Scripting	An abnormal process is opened by a scripting tool.
Abnormal Process Created a Remote Thread in a Windows	PowerShell & Scripting	An abnormal process is injected into a known windows process .
Multiple Distinct Reconnaissance Tools Executed	Discovery & Reconnaissance	Multiple reconnaissance tools are executed in an hour.
Multiple Reconnaissance Tool Activities Executed	Discovery & Reconnaissance	Multiple reconnaissance tool activities are executed in an hour.
Process Executed Multiple Times by a Reconnaissance Tool	Discovery & Reconnaissance	A reconnaissance tool executed a process multiple times.
User Ran an Abnormal Process to Execute a Scripting Tool	PowerShell / Scripting	An abnormal process is executed a scripting tool.
User Ran a Scripting Tool that Triggered an Abnormal Application	PowerShell / Scripting	An abnormal scripting tool is executed for an abnormal application.
User Ran a Scripting Tool to Open an Abnormal Process	PowerShell / Scripting	An abnormal scripting tool is executed for 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	When an IP address in the organization sends an unexpectedly high amount of data to an SSL Subject.
Abnormal Traffic Volume Sent from IP to Domain	SSL Subject	Data exfiltration	When an IP address in the organization sends an unexpectedly high amount of data to a domain and SSL Subject.
Abnormal Traffic Volume Sent from IP to Organization	SSL Subject	Data exfiltration	When an IP address in the organization sends an unexpectedly high amount of data to an organization and SSL Subject.
Abnormal Traffic Volume Sent from IP to Port	SSL Subject	Data exfiltration	When an IP address in the organization sends an unexpectedly high amount of data to a port and SSL Subject.
Abnormal Traffic Volume Sent to SSL Subject	SSL Subject	Data exfiltration	When an unexpectedly high amount of data is sent to an SSL Subject.
Abnormal Traffic Volume Sent to Domain	SSL Subject	Data exfiltration	When an unexpectedly high amount of data is sent to a domain and SSL Subject.
Abnormal Traffic Volume Sent to Port	SSL Subject	Data exfiltration	When an unexpectedly high amount of data is sent to a port and SSL Subject.

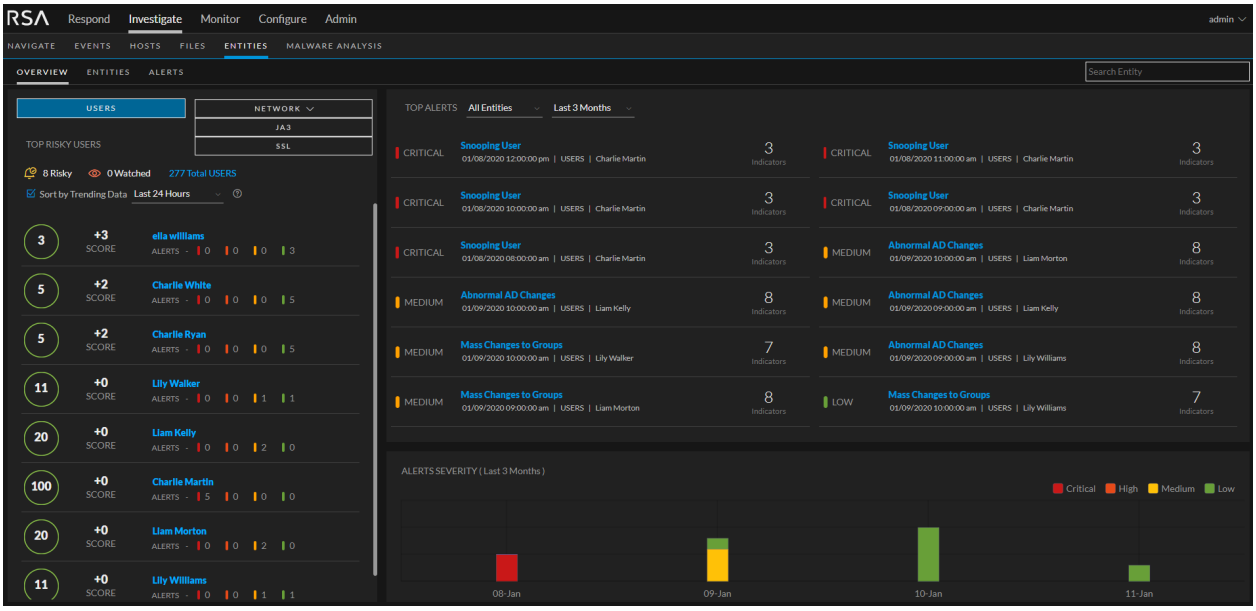
Indicator	Entity Type	Alert Type	Description
Abnormal Traffic Volume Sent to Organization	SSL Subject	Data exfiltration	When an unexpectedly high amount of data is sent to an organization and SSL Subject.
Abnormal Traffic Volume Sent from JA3	JA3	Data exfiltration	When a client application sends an abnormally high amount of data.
High Number of IPs Use JA3	JA3	Phishing	When a client application abnormally sends high number of IPs which use JA3.
Abnormal SSL Subject for Source Netname	SSL Subject and JA3	Data exfiltration	When a source netname contacts an abnormal SSL Subject.
Abnormal Domain for Source Netname	SSL Subject and JA3	Data exfiltration	When a source netname contacts an abnormal domain.
Abnormal Destination Port for Source Netname	SSL Subject and JA3	Data exfiltration	When a source netname contacts an abnormal destination port.
Abnormal Organization for Source Netname	SSL Subject and JA3	Data exfiltration	When a source netname contacts an abnormal organization.
Abnormal Country for SSL Subject	SSL Subject and JA3	Data exfiltration	When an SSL Subject is contacted with an abnormal destination country.
Abnormal Destination Port for SSL Subject	SSL Subject and JA3	Data exfiltration	When an SSL Subject is contacted through an abnormal destination port.
Abnormal Time for SSL Subject	SSL Subject and JA3	Non-Standard Hours	When an SSL Subject is contacted at an abnormal time.
Abnormal Destination Port for Domain	SSL Subject and JA3	Data Exfiltration	When a domain is accessed through an abnormal destination port.
Abnormal Destination Port for Organization	SSL Subject and JA3	Data Exfiltration	When an organization is accessed through an abnormal destination port.
Abnormal Time for JA3	SSL Subject and JA3	Non-Standard Hours	When a client application is contacted at an abnormal time.
Abnormal JA3 for Source Netname	SSL Subject and JA3	Phishing	When a source netname utilizes an abnormal client application.
Abnormal SSL Subject for JA3	SSL Subject and JA3	Phishing	When a client application contacts an abnormal SSL Subject.
Abnormal Domain for JA3	SSL Subject and JA3	Phishing	When a client application contacts an abnormal domain.

Indicator	Entity Type	Alert Type	Description
Abnormal Destination Port for JA3	SSL Subject and JA3	Phishing	When a client application contacts an abnormal destination port.

Access NetWitness UEBA

Note: To access the NetWitness UEBA service and Entities 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*. You must also ensure that you have proper NetWitness UEBA licensing configured. For information about NetWitness UEBA licensing, see the "User and Entity Behavior Analytics License" topic in the *Licensing Management Guide*.

To access NetWitness UEBA, log into NetWitness Platform and go to **INVESTIGATE** > **ENTITIES**. The Entities view, which contains all the NetWitness UEBA feature is displayed.



You can choose a dark or a light theme for the view. For information, please see the "Choose the Appearance of NetWitness Platform" topic in the *RSA NetWitness Getting Started Guide*.

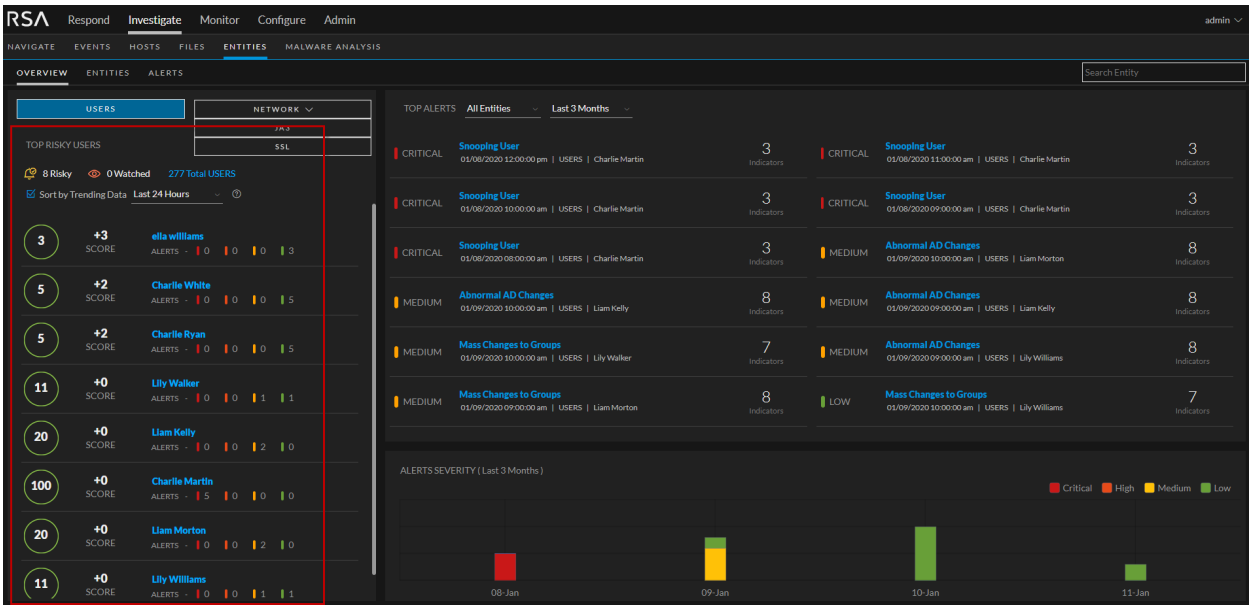
Investigate High-Risk User or Network Entity

A user or entity score is built based on the alert score and the alert severity. Using the user or network entity score, you can identify the users and network entities that require immediate attention, perform deeper investigation, and take required action. The UI is divided into three tabs namely **OVERVIEW** tab, **ENTITIES** tab and **ALERTS** tab. You can identify high-risk users or network entities from either the **OVERVIEW** tab or the **ENTITIES** tab and view the top risky alerts in the **ALERTS** tab.

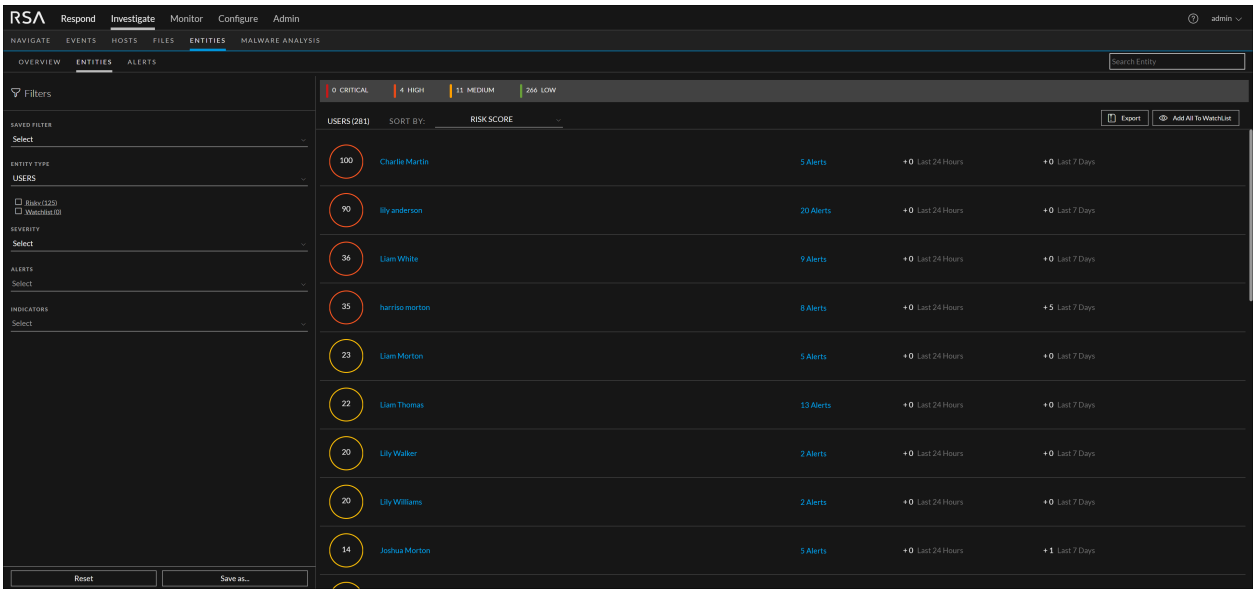
In the **OVERVIEW** tab select **USERS** to investigate on the top risky users or select **NETWORK** to investigate on the top risky network entities. The **OVERVIEW** tab is further divided into three different panels as follows:

- Top Risky Users or Network Entities - This panel displays the number of risky user or network entities, number of watched user or network entities, total number of user or network entities. The results in this panel can be sorted by the user or network entity score, trending data score or alert severity.
- Top Alerts - This panel displays a list of top alerts of last 24 hours, last seven days, last one month ore last three months. Each item provides further details such as name of the user or network entity and number of associated indicators.
- Alert Severity - This panel displays the alert severity for the last three months in a bar diagram which can be filtered by clicking on Critical, High, Medium or Low check boxes.

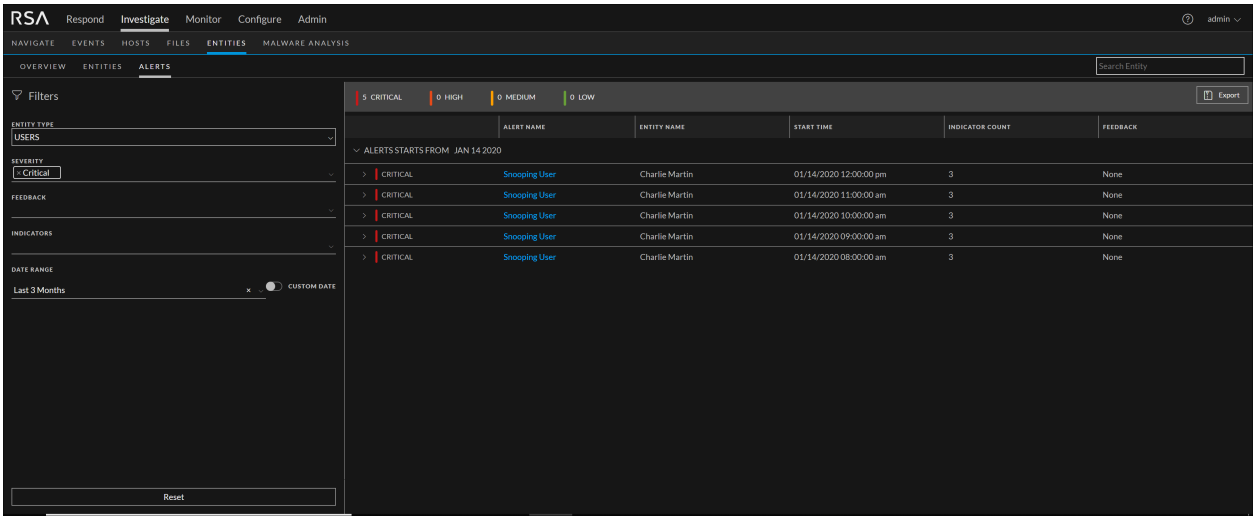
For example, the following figure displays the top ten high-risk users in the **OVERVIEW** tab.



The following figure is an example of all the risky users in your environment in the **ENTITIES** tab.



The following figure is an example of the risky user alerts in your environment in the **ALERTS** tab.



The following is a high-level process to investigate high-risk users or entities in your environment.

1. Identify high-risk users. You can identify high-risk users using the following ways:
   - The **OVERVIEW** tab shows the top ten risky users in your environment. From the listed users identify the users with a critical severity or user score more than 100.
   - The **ENTITIES** tab shows all the risky users in your environment, you can sort by Risk Score (default), Name, Alerts, Trending LastDay, Trending LastWeek. Identify how many users are marked Critical, High and Medium or based on the forensic investigation, identify malicious user behavior and build use-case driven target user lists using behavioral filters. Additionally, you can also use different types of filters (Risky or Watchlist) to identify targeted group of high-risk users.
   - The **ALERTS** shows all the risky users alerts in your environment. You can sort by Critical, High, Medium or Low. Click the Export button to download the alert report in .

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

For more information, see the Identify High-Risk User or Network Entity 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 User Or Network 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 User or Network Entity topic.

Identify High-Risk User or Network Entity

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

- View top ten 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 User or Network Entities

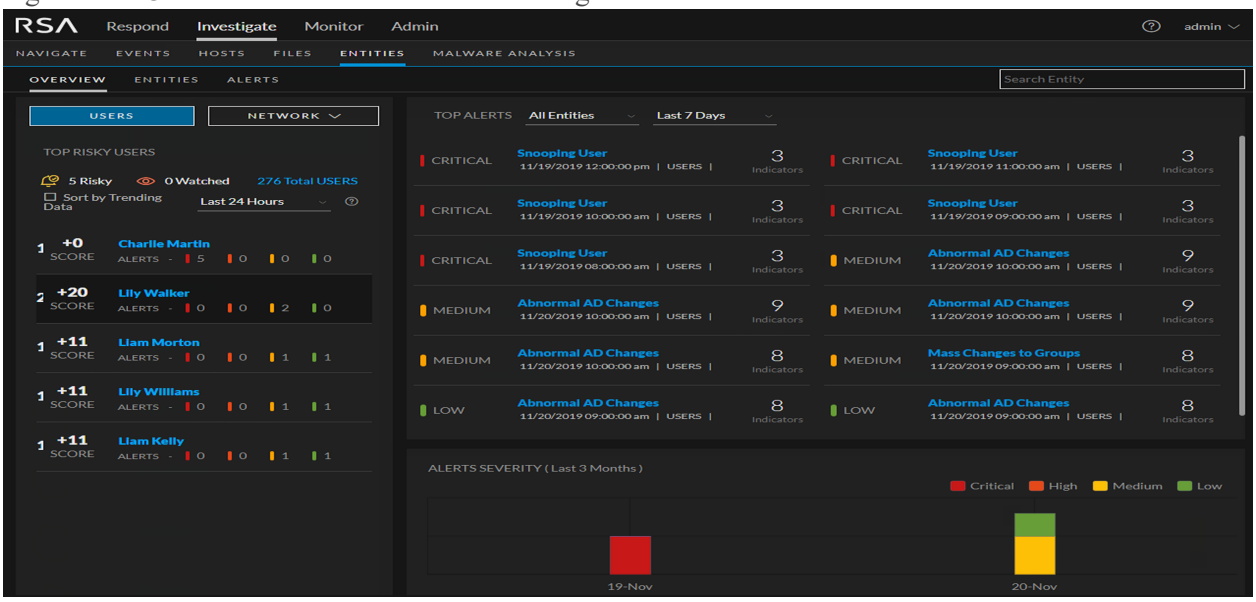
In the **OVERVIEW** tab, you can view the list of top ten high-risk user or network entities in your environment along with the risky score.

To view the top risky entities:

Log into **NetWitness Platform** and go to **Investigate** > **ENTITIES**.
The Overview tab is displayed with the high-risk user or network entities.

To view the high risk users, click the **Users** tab.

To view the high risk network entities, click the **Network** tab. Select JA3 from the drop-down to view high-risk JA3 entities. Select SSL to view the high risk SSL entities.



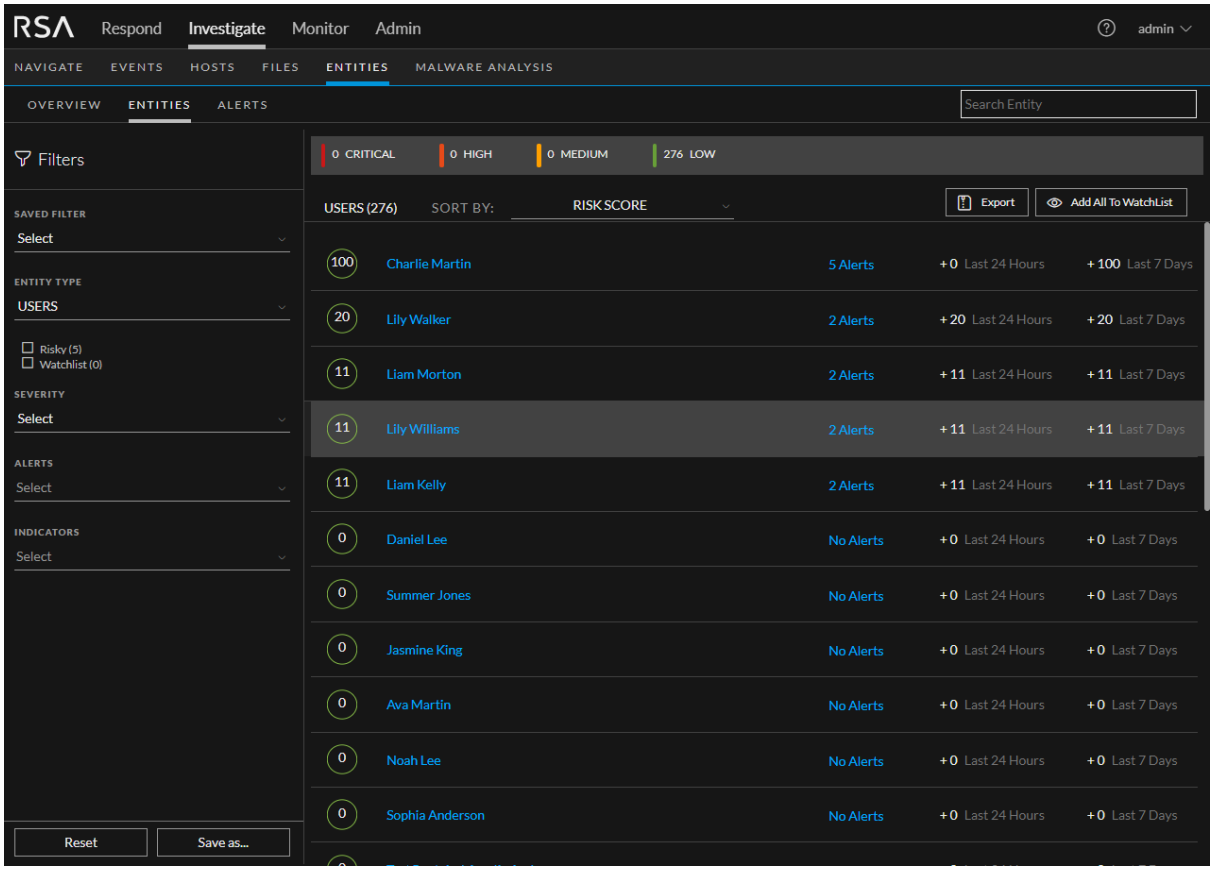
View All High-Risk User or Network Entities

In the **ENTITIES** tab, you can view the list of all the high risk user or network entities in your environment along with the user or network entity score and total number of alerts associated with the user or network entities.

To view all high-risk user or network entities:

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

2. Click **ENTITIES** tab.
   The list of all high-risk user or network entities is displayed.

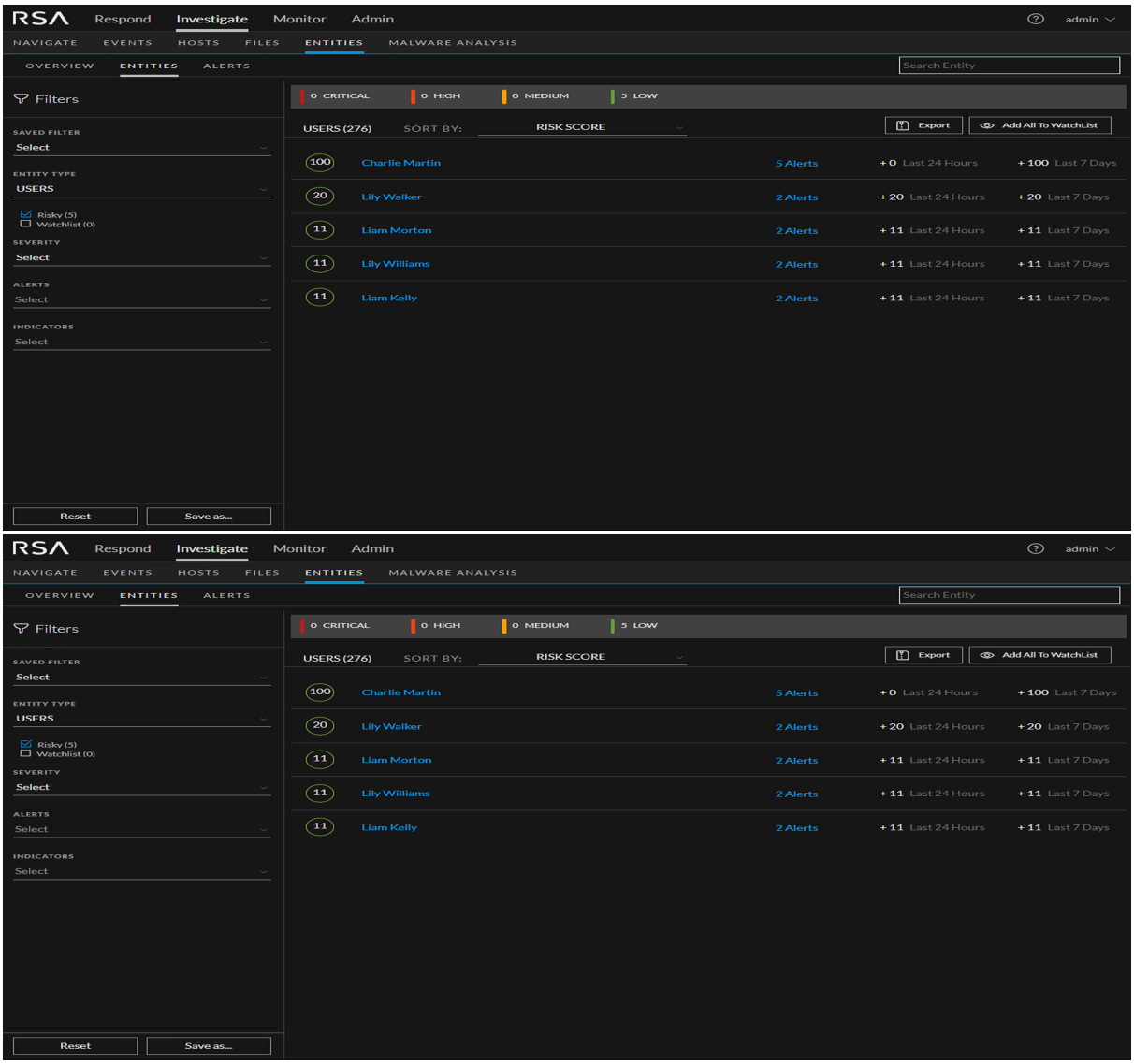


View User or Network Entities of a Specific Group

In the **ENTITIES** tab, you can use different types of filters to identify targeted group of high-risk user or network entities.

To view users of specific group:

1. Log into **NetWitness Platform** 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 user or network entities in your environment, select **Risky** in the left pane.
     All the risky user or network entities along with their user or network entity score is 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 or network entities of one or more group by selecting one or more filters. For example, if you want to view the list of risky user or network entities, select the **Risky** and **Watchlist** filters.

View Users Based on Forensic Investigation

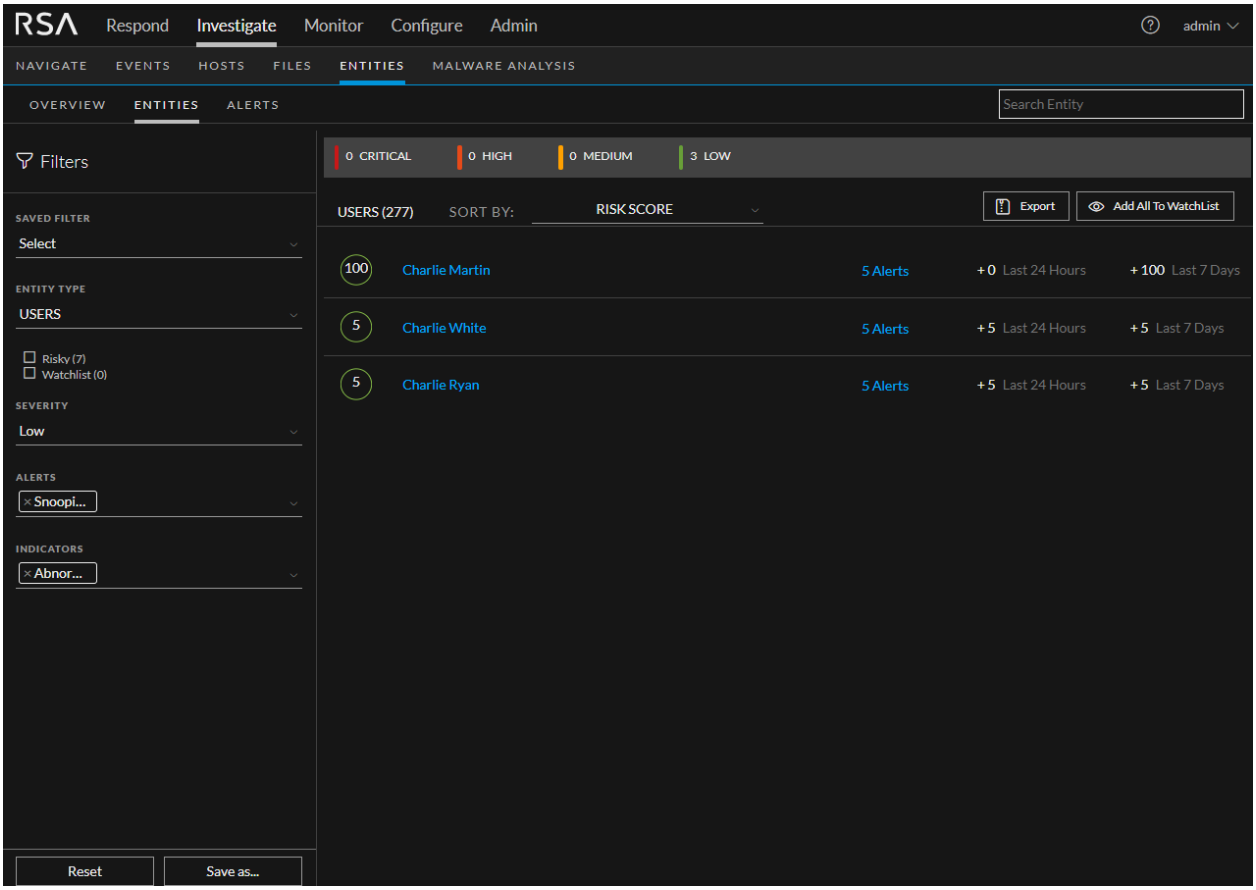
In the **ENTITIES** tab, you can use Alert Types and Indicators which are behavioral filters to view high-risk user or network entities based on forensic investigation. For more information on forensic investigation, see *Forensic Workflow* in the Introduction topic.

To view users based on specific forensic investigation:

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

3. To filter the result for user or network entity, select Users or JA3 or SSL in the **ENTITY TYPE** drop-down list.
4. To filter the result for severity, select Severity in the **SEVERITY** drop-down list.
5. To create a behavioral filter using alert types, select one or more alerts in the **ALERTS** drop-down list.
6. To create a behavioral filter using indicators, select one or more indicators in the **INDICATORS** 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 files and theft of sensitive data, you can create a behavioral filter with Alert Types = **Abnormal File Access** and Indicators = **Abnormal File Access Time**.



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

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

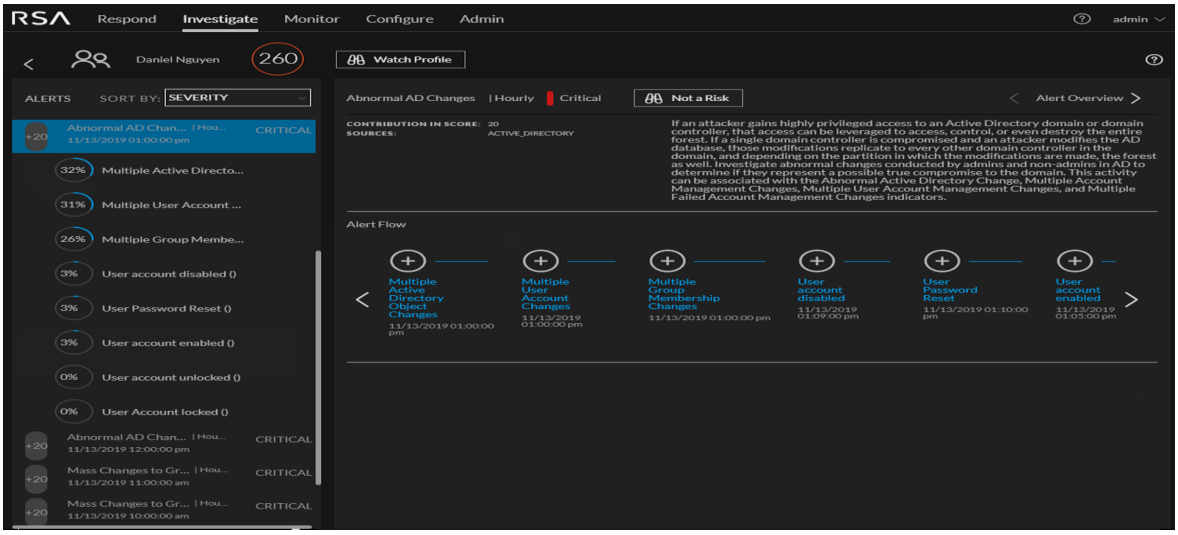
Similarly, you can view other entities such as JA3 and SSL based on forensic investigation.

Begin an Investigation of High-Risk User Or Network Entity

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

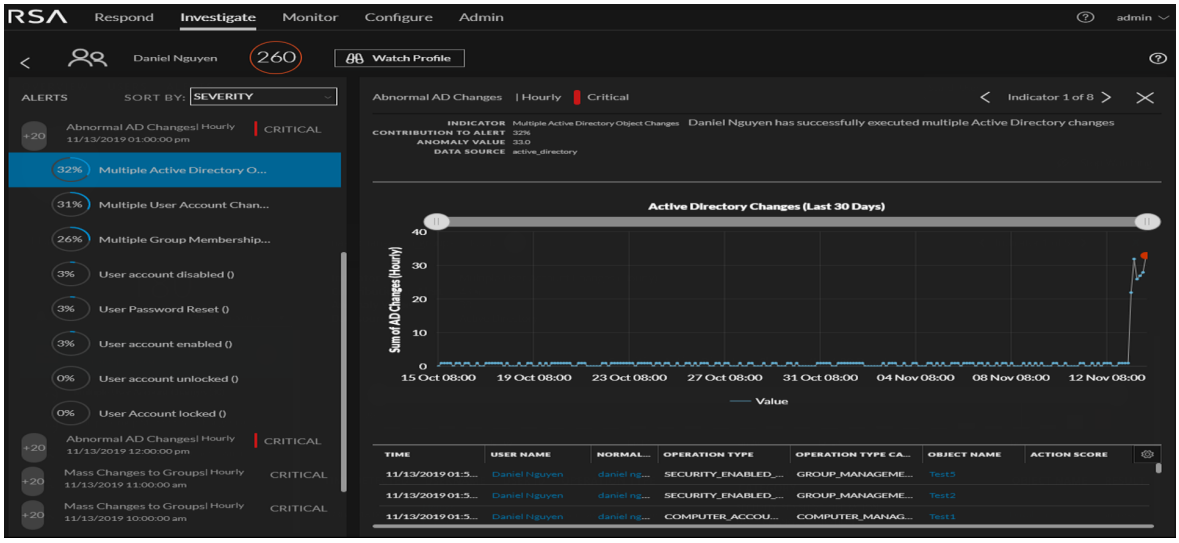
To investigate high-risk user or network entities:

1. Log into **NetWitness Platform** and go to **INVESTIGATE** > **ENTITIES**. Do any of the following:
   a. In the **Overview** tab, in the **High Risk Users** panel, click a username you want to investigate.
   The User Profile view is displayed.
   b. In the **ENTITIES** tab, Click on the username you want to investigate.
   The User Profile view is displayed.
2. To investigate the alerts of the user, click the alert name in the **ALERTS** panel. The following information is displayed:
   - The alert name
   - The timeframe of the alert (Hourly)
   - The severity level icon
   - The contribution in score (for example, +20)
   - The data sources for the alert (for example, Logon)
   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 of a user, in the **ALERTS** 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.



Take Action on High-Risk User or Network Entity

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

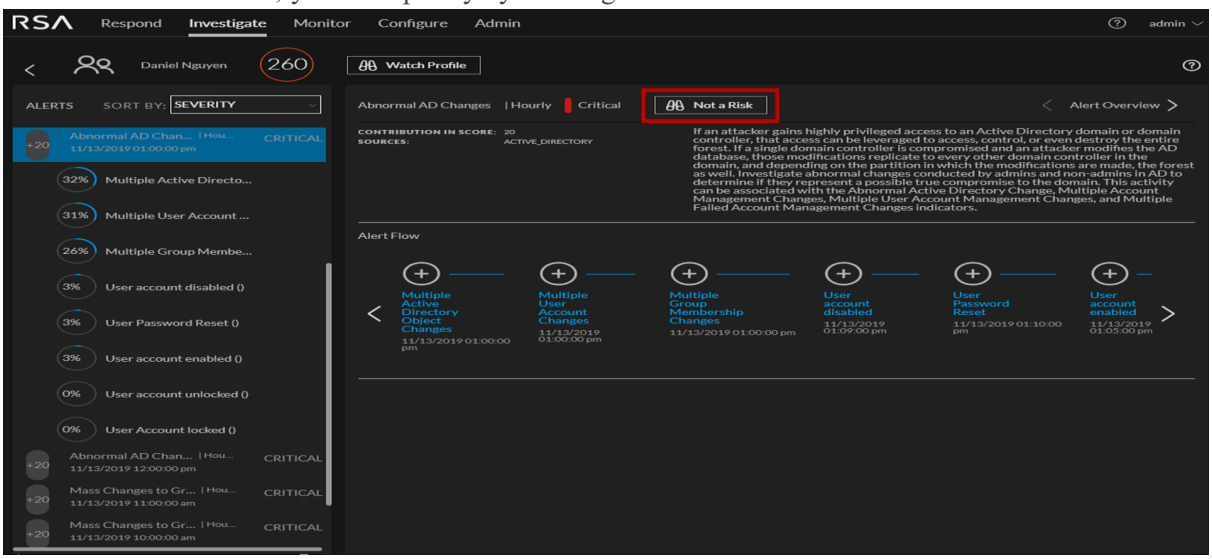
- Specify if the alert is not risky
- Save the behavioral profile for the use case found in your environment
- Add user or network entities to the watchlist, and the watch user or entity profile, if you want to keep a track of the user or entity activity

Specify that an alert is not risky.

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

To specify if the alert is not risky:

1. Log into **NetWitness Platform** and go to **Investigate** > **ENTITIES**.
2. Take action on the user or network entity from any of the following tabs:
   a. In the **OVERVIEW** tab, in the **Top Risky Users** panel, click on the username.
   The User Profile view is displayed.
   b. In the **ENTITIES** tab, 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.

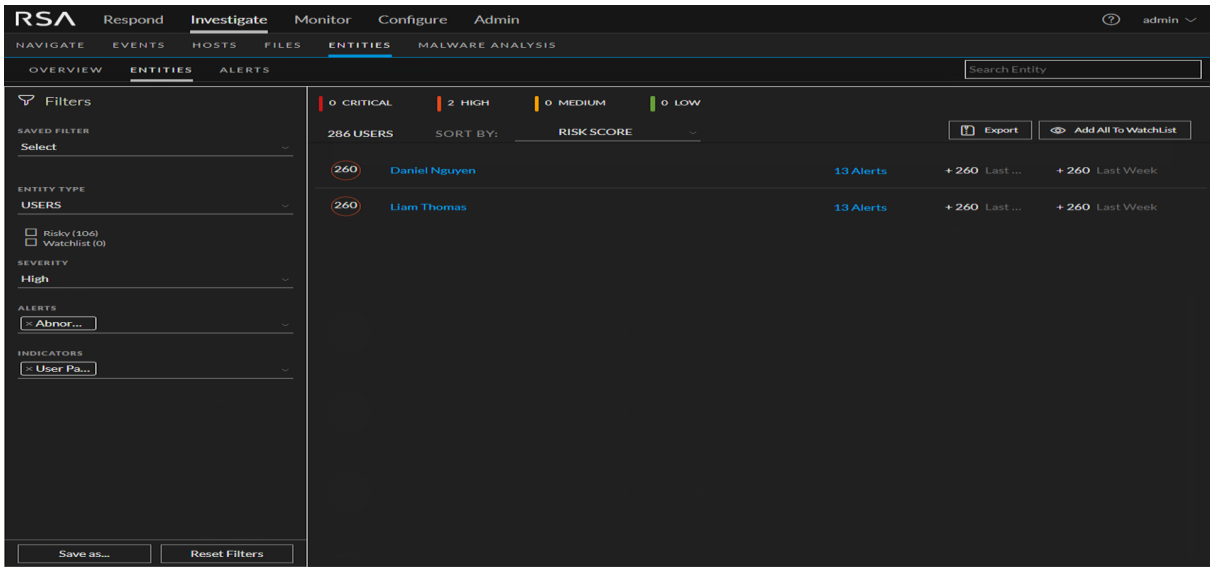
Save Behavioral Profile

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.

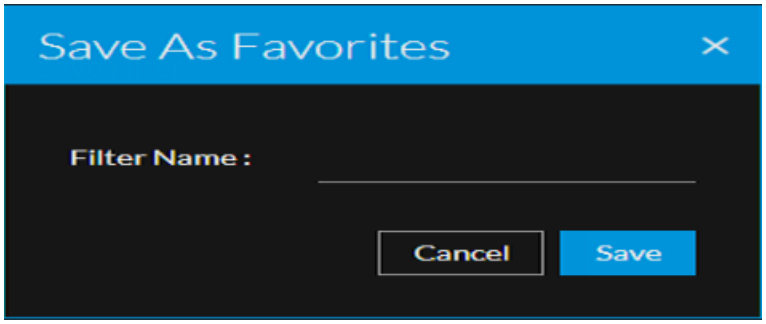
For example, if your organization is attacked and the attackers penetrated by brute forcing user accounts for users , you can select filters using the brute force alert type. This can be saved as favorite. You can proactively monitor for future brute force attempts. To do so, you can click the favorite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

To save a behavioral profile:

1. Log into **NetWitness Platform** and go to **Investigate** > **ENTITIES**.
   The Overview tab is displayed.
2. Click the **ENTITIES** tab.
3. In the **Filters** panel, select the following.
   1. Entity in the **ENTITY TYPE** drop-down.
   2. Severity in the **SEVERITY** drop-down,
   3. Alert in the **ALERTS** drop-down.
   4. Indicators in the **INDICATORS** drop-down.
4. Click **Save as...**.



5. In the **Save As Favorites** dialog, enter the filter name and click **Save**.



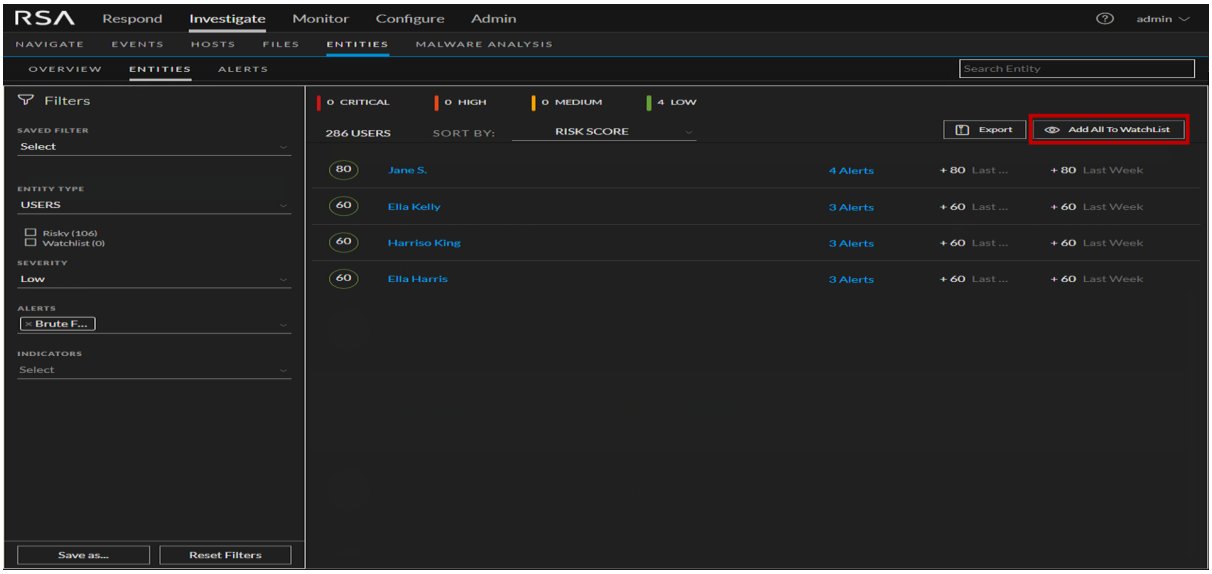
The behavioral profile is saved and displayed in the **SAVED FILTER** drop-down.

Add All Users or Entities to the Watchlist

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

To add all user or network entities to the watchlist:

1. Log into **NetWitness Platform** and go to **Investigate** > **ENTITIES**.
   The Overview tab is displayed.
2. Select the **ENTITIES** tab.
3. In the Filters panel, Apply the filters.
   A list of users for the applied filters is displayed in right pane.
4. Click **Add All to Watchlist**.



The list of users is added to the watchlist.

Watch Profile

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

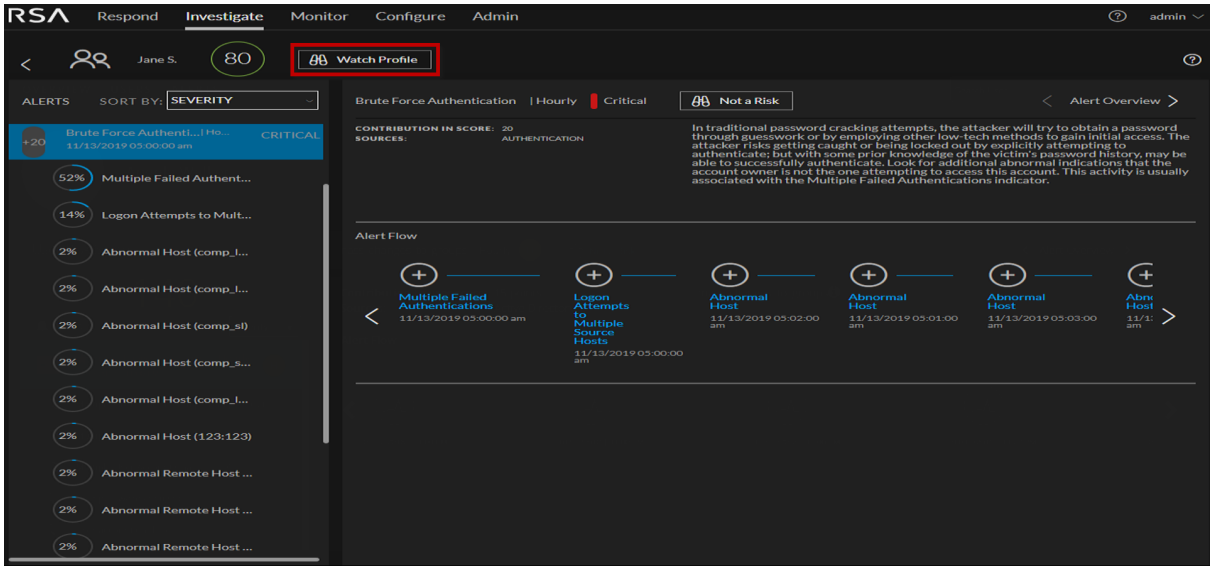
To watch user profile:

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

   a. In the **Overview** tab, under **Top Risky Users** panel, click on the username.
   The User Profile view is displayed.

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

2. Click **Watch Profile**.



The user is added to the watchlist. Similarly, you can watch profiles for network entities.

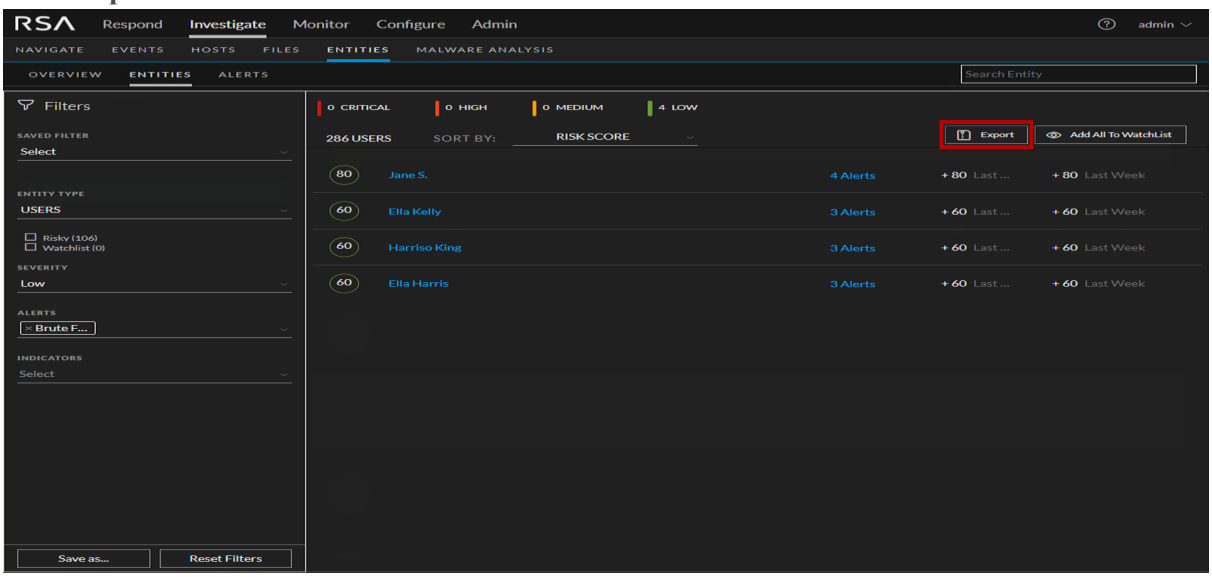
Export a list of High-Risk User or Network Entity

You can export a list of all user or network entities 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** > **ENTITIES**.
   The Overview tab is displayed.
2. Select the **ENTITIES** tab.

3. Click **Export**.

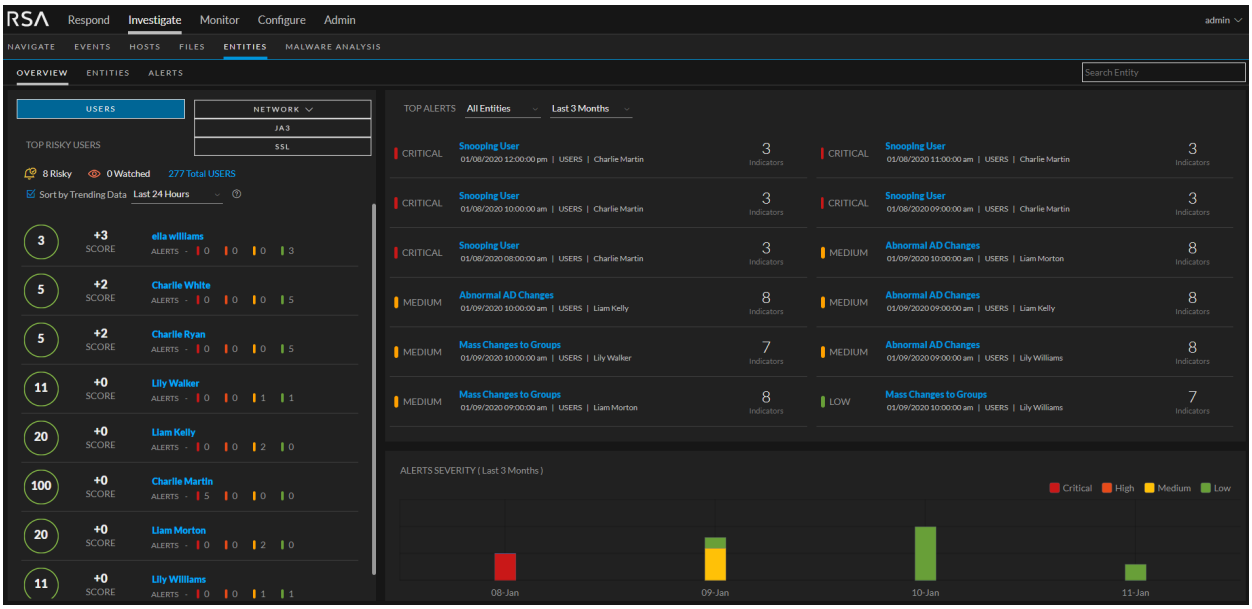


The list of all user and network entities and the associated scores is downloaded in the .csv file format.

Investigate Top Alerts

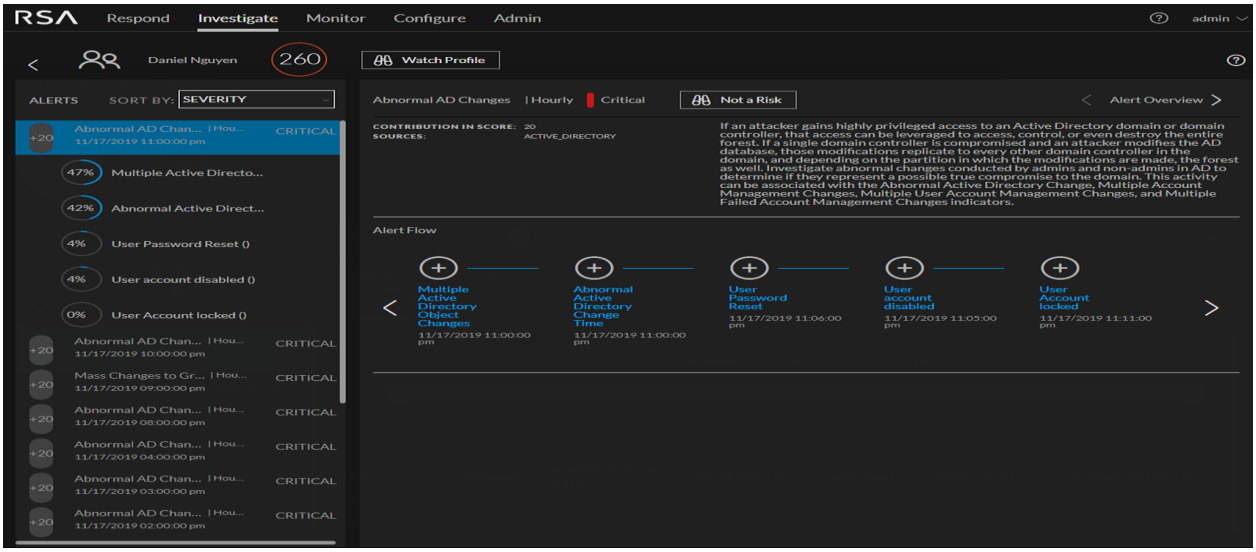
Anomalies that are found as incoming events are compared to the baseline and compiled into hourly alerts. Relatively strong deviations from the baseline, together with a unique composition of anomalies, are more likely to get a higher alert score.

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.

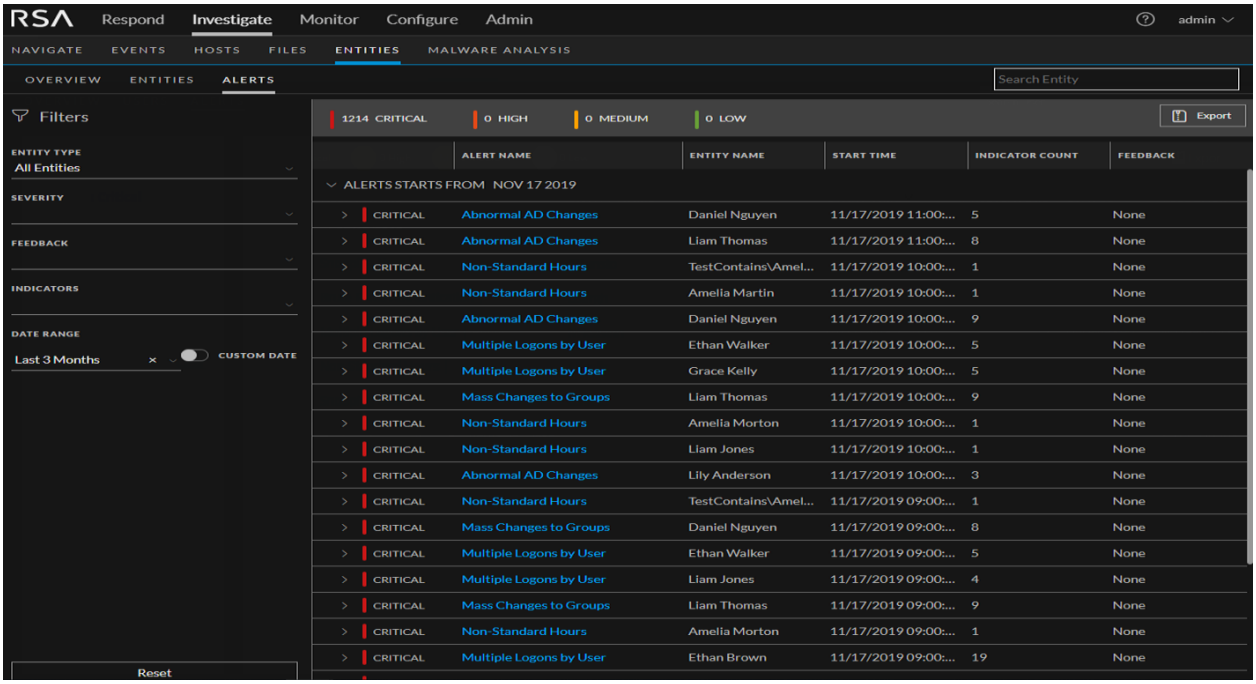


To investigate an alert on this page, click an alert in the **Top Alerts** section to see details about the alert.

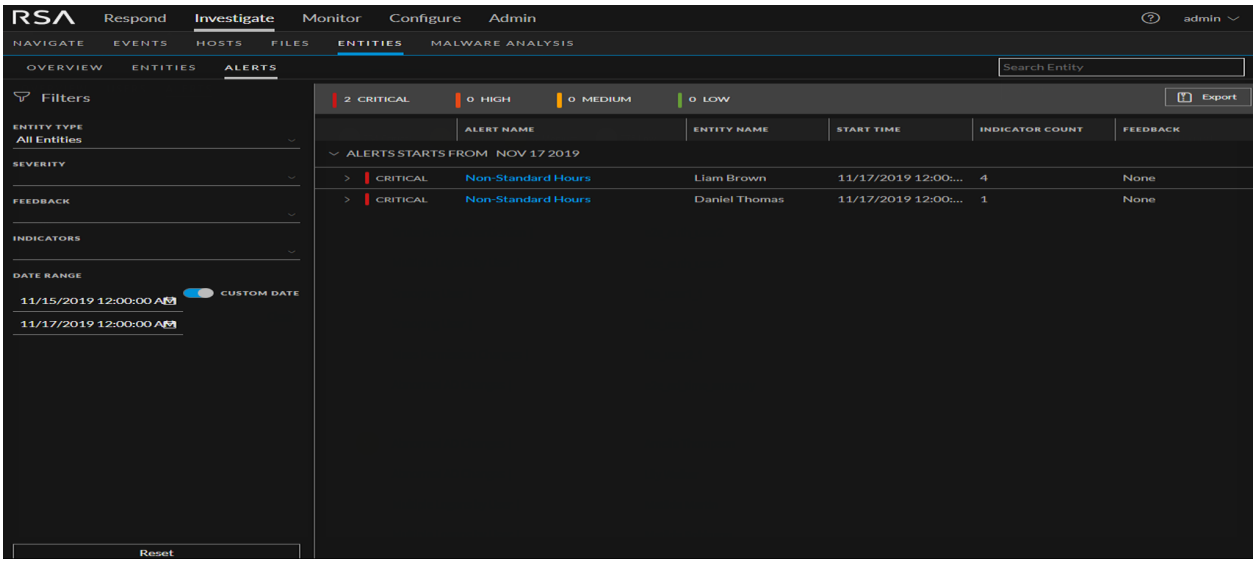
The following figure shows details about the event that caused the alert, and the timeframe in which it occurred.



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.



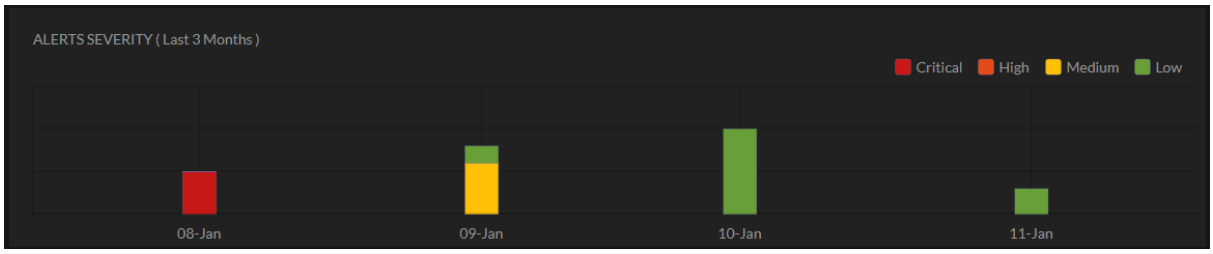
Investigating alerts is particularly useful when you want to focus on a timeframe in which you believe your systems were compromised. You can view forensic information based on a timeframe and gather detailed information about events that occurred during that time in the Alerts tab.



Begin an Investigation of Critical Alerts

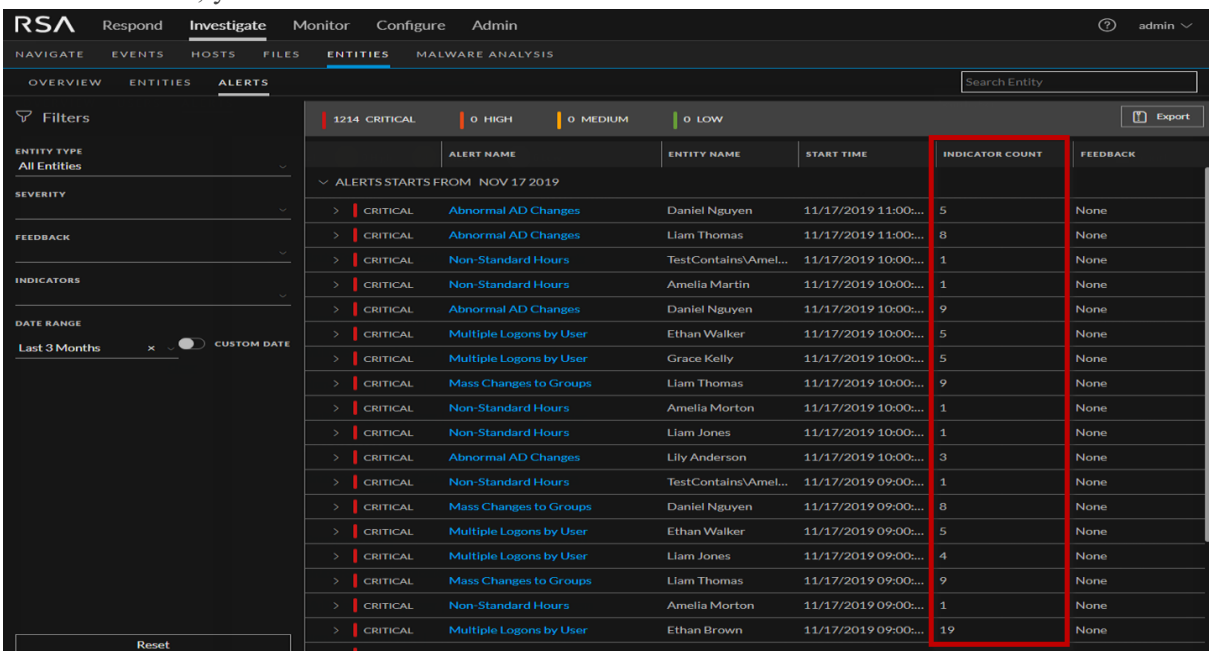
You can begin your investigation of critical alerts in the following ways:

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).

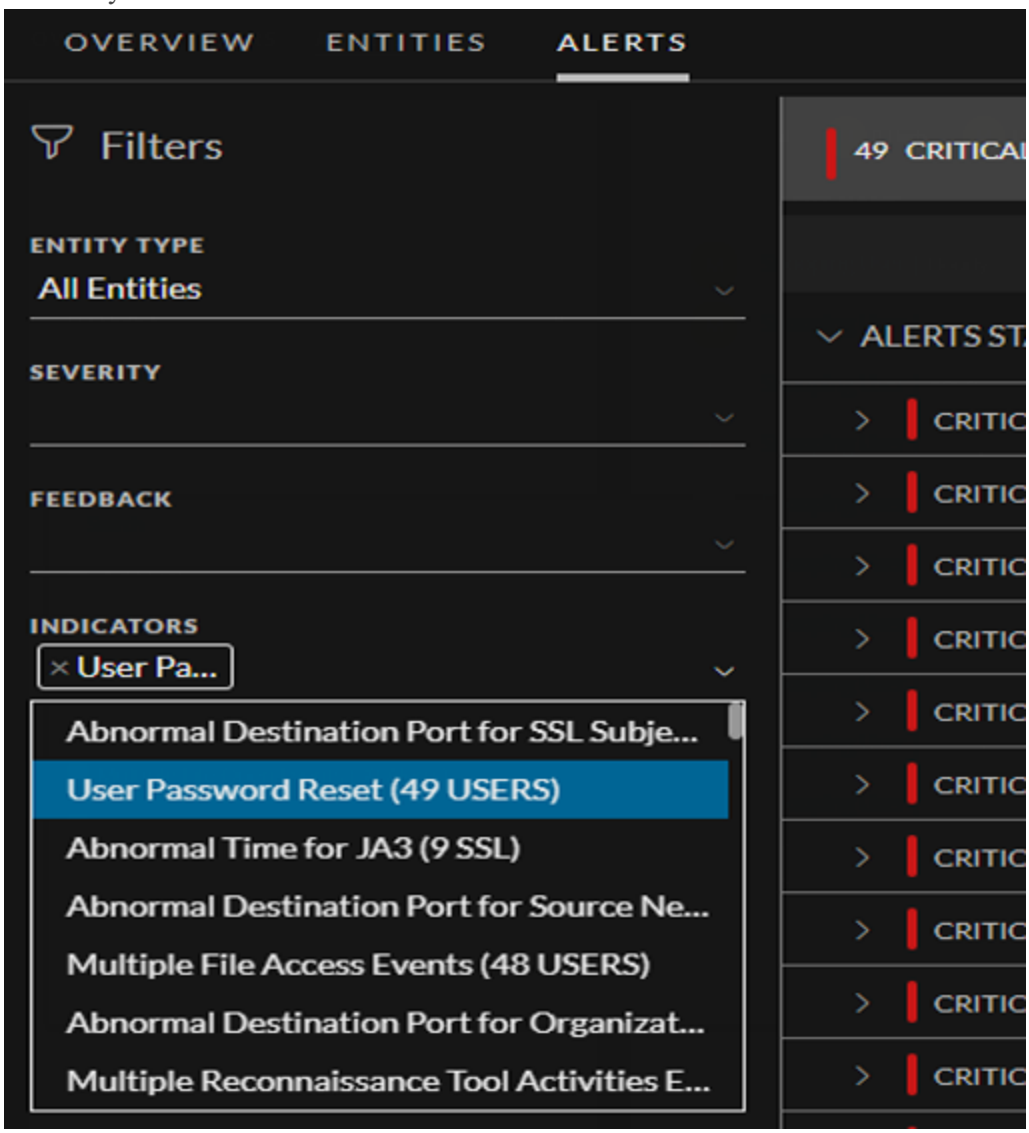
2. In the Alerts tab, you can view the indicator count:



   To identify the users with the highest number of alerts, more indicators help illustrate a more interesting story and provide you with a more solid 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 activity that a human can perform manually (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 fact that the strongest contributing indicator 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 what could explain the observed behaviors.

- Follow up by reviewing each indicator and demonstrating how supporting information, in the form of graphs and events, can help analysts 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 your investigation of alerts. For more information, see Take Action on High-Risk User or Network Entity .

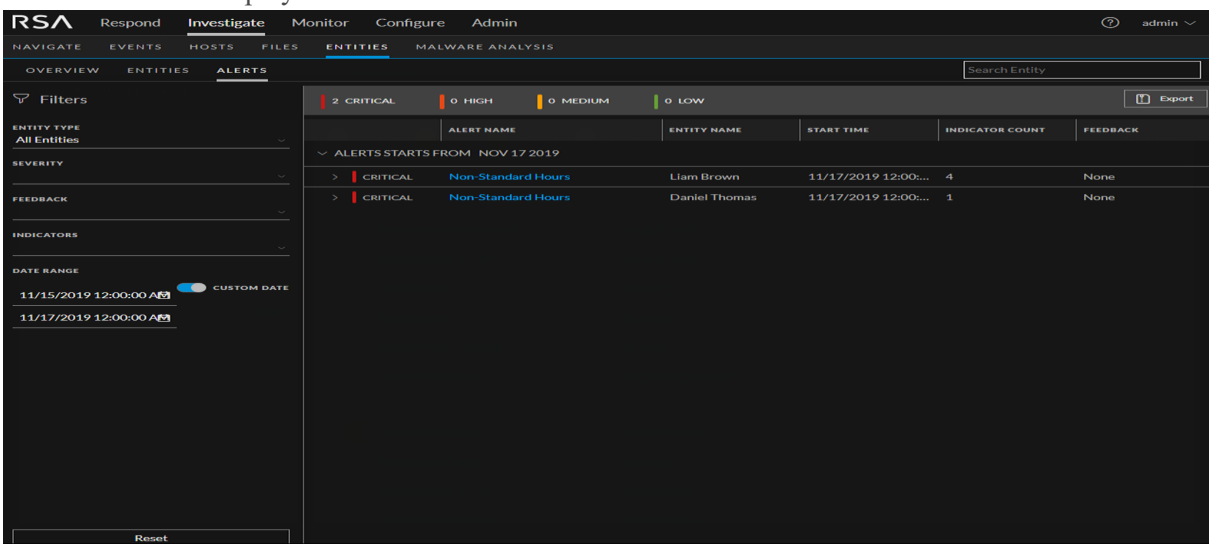
The following topics explain various ways to investigate alerts.

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

Filter Alerts

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

1. Log into NetWitness Platform and go to **INVESTIGATE** > **ENTITIES** > **Alerts**.
   The Alerts tab is displayed.



2. To filter by severity, click the don arrow under **SEVERITY** in the **Alerts Filters** panel, select any one option. The options are Critical, High, Medium, and Low.
3. To filter by feedback, click the down arrow under **FEEDBACK**, select any one option. The options are None, and Rejected.
4. To filter by entity, click the down arrow under **ENTITY TYPE**, 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 pane according to the filter you selected. To reset filters, in the bottom of left pane , click **Reset**.

Investigate Events

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

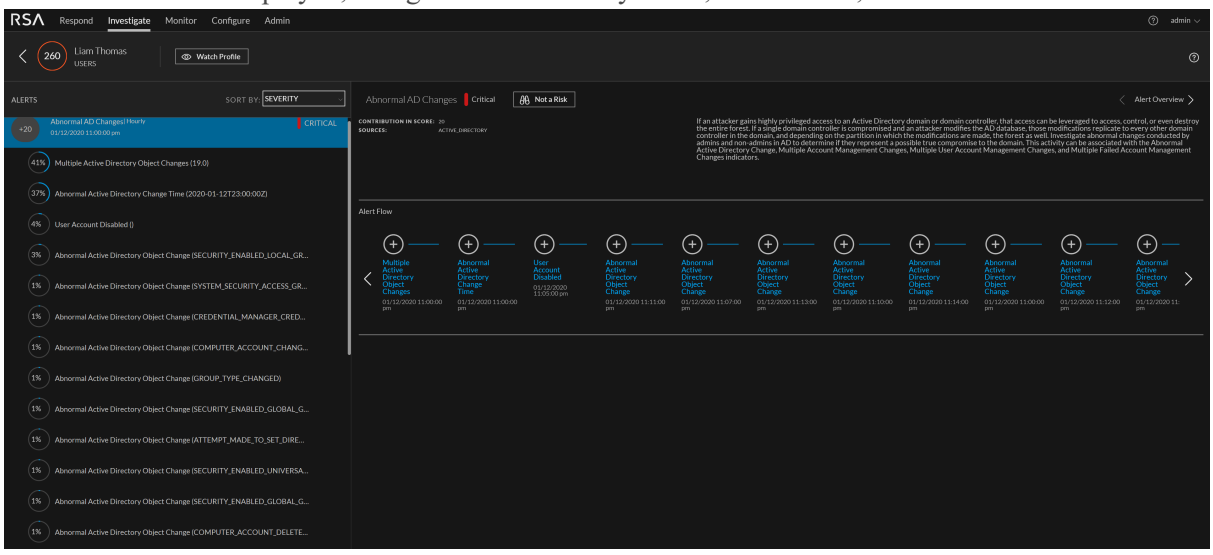
In the events table you can find all the events contributed to the specific indicator for the specific user or network entity.

For example, you can further investigate on events by clicking on a Username that enables Pivot to **Investigate** > **Events**. In the Events view, you can see the list of events that occurred on that day for the specific user. By default the time range is set to one day. 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.

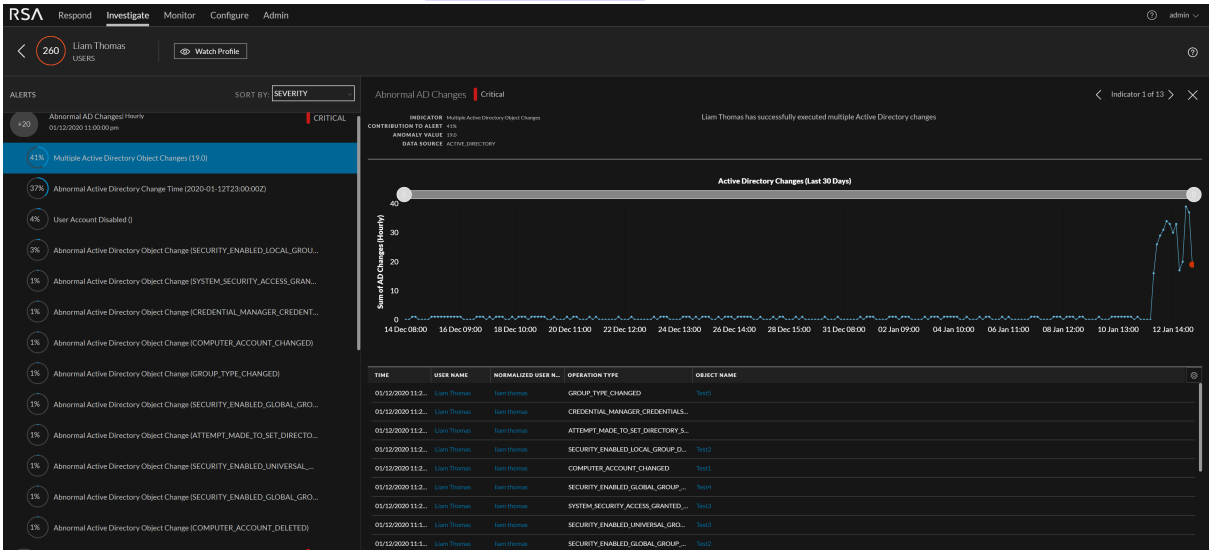
To view the events:

1. Log into NetWitness Platform and go to **Investigate** > **ENTITIES** > **ALERTS**.
2. Under **ALERTS STARTS FROM** date, click an alert name.
   The indicators are displayed, along with the anomaly value, data source, and start time.



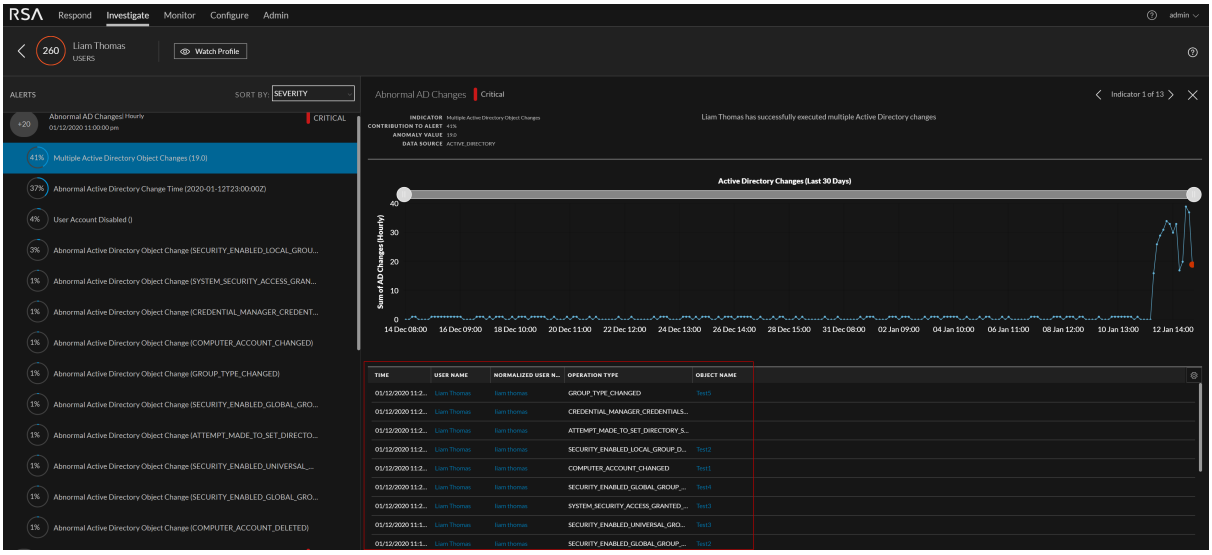
3. Under **Alert Flow**, click on the  icon.
   A graph is displayed that shows details about a specific indicator, including the timeline in which the

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 Profile View.



To pivot to the Events view:

1. Go to **Investigate** > **ENTITIES**, and select an alert or a user.
2. Under **ALERTS**, select an alert name.
   Indicators are displayed under the alert.
3. Select an indicator of interest.
   Values that can be used to pivot are highlighted in light blue at the bottom of the panel.



4. In the Events table, click the username highlighted in blue.
   The Events view is displayed.

For information about investigating items of interest in the Events view, see "Investigating Raw Events in the Events View" 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 **Investigate** > **ENTITIES**, and select an alert or a user.
2. Under **ALERTS**, 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 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 **Investigate** > **ENTITIES**, and select an alert or a user.
2. Under **ALERTS**, 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.

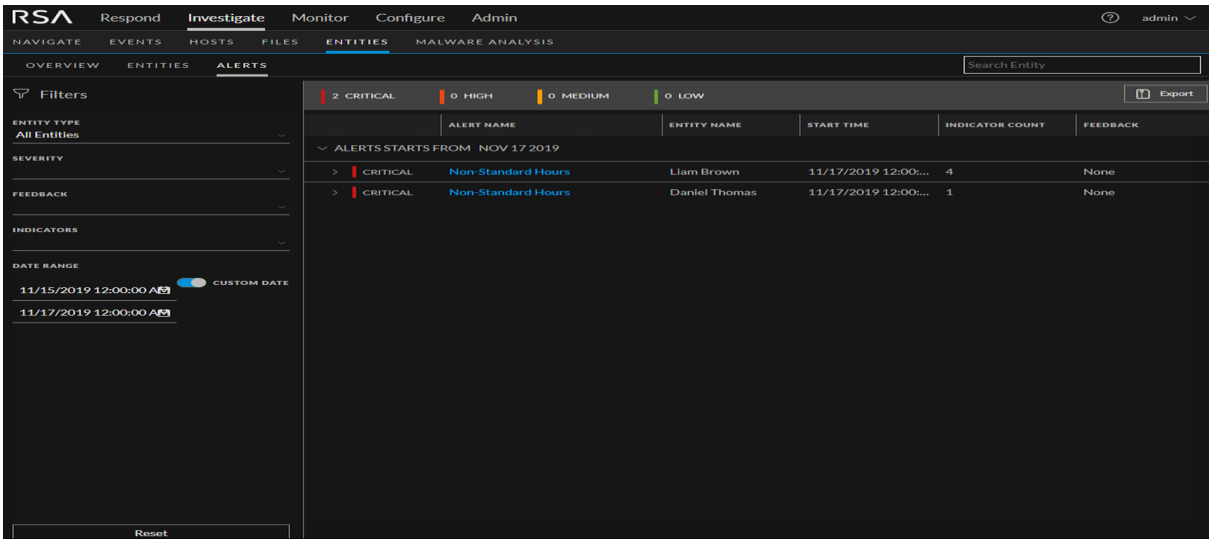
For more information, see "Investigating a Process" topic in the *NetWitness Endpoint User Guide*.

Manage Top Alerts

You can export a list of all alerts to a .csv file format. An analyst 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. Log into NetWitness Platform and go to **Investigate** > **ENTITIES** > **ALERTS**.
   The Alerts tab is displayed.


RSA
Respond
Investigate
Monitor
Configure
Admin
admin
NAVIGATE
EVENTS
HOSTS
FILES
ENTITIES
MALWARE ANALYSIS
OVERVIEW
ENTITIES
ALERTS
Search Entity
Filters
ENTITY TYPE
All Entities
SEVERITY
FEEDBACK
INDICATORS
DATE RANGE
11/15/2019 12:00:00 AM
CUSTOM DATE
11/17/2019 12:00:00 AM
Reset
2 CRITICAL
0 HIGH
0 MEDIUM
0 LOW
Export
ALERT NAME
ENTITY NAME
START TIME
INDICATOR COUNT
FEEDBACK
ALERTS STARTS FROM NOV 17 2019
CRITICAL
Non-Standard Hours
Liam Brown
11/17/2019 12:00:...
4
None
CRITICAL
Non-Standard Hours
Daniel Thomas
11/17/2019 12:00:...
1
None

2. At the top right, click **Export**.
   All the alert data is downloaded in a .csv file format. Here is an example of the exported alert data in .csv format:

	A	B	C	D	E	F	G
1	Alert Name	Entity Name	Start Time	# of Indica	Status	Feedback	Severity
2	Brute Force Authenticati	e2e_auth_user2	Mar 06 20	1	Reviewed	No Feedback	Low
3	Multiple Logons by User	e2e_auth_user3	Mar 06 20	1	Reviewed	No Feedback	Low
4	Snooping User (Hourly)	file_user1_1	Mar 06 20	2	Reviewed	No Feedback	Low
5	Snooping User (Hourly)	file_user3_1	Mar 06 20	1	Reviewed	No Feedback	Low
6	Mass Permission Change	file_user2_1	Mar 06 20	1	Reviewed	No Feedback	Low
7	Abnormal AD Changes (H	e2e_ad_time_anor	Mar 06 20	4	Reviewed	No Feedback	Low
8	Abnormal AD Changes (H	Amelia Thompson	Mar 05 20	13	Reviewed	No Feedback	Medium
9	Abnormal AD Changes (H	Lily Walker	Mar 05 20	11	Reviewed	No Feedback	Low
10	Multiple Logons by User	Matilda Martin	Mar 05 20	6	Reviewed	No Feedback	Low
11	Multiple Logons by User	Matilda Robinson	Mar 05 20	6	Reviewed	No Feedback	Low

View NetWitness UEBA Metrics in Health and Wellness

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

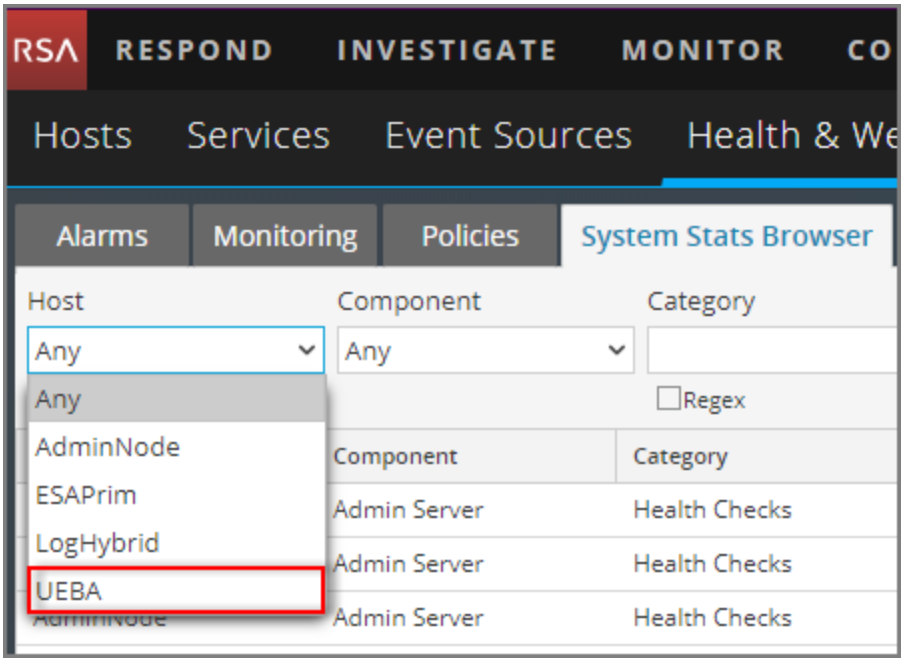
Analysts can use these metrics in the following ways:

- 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.

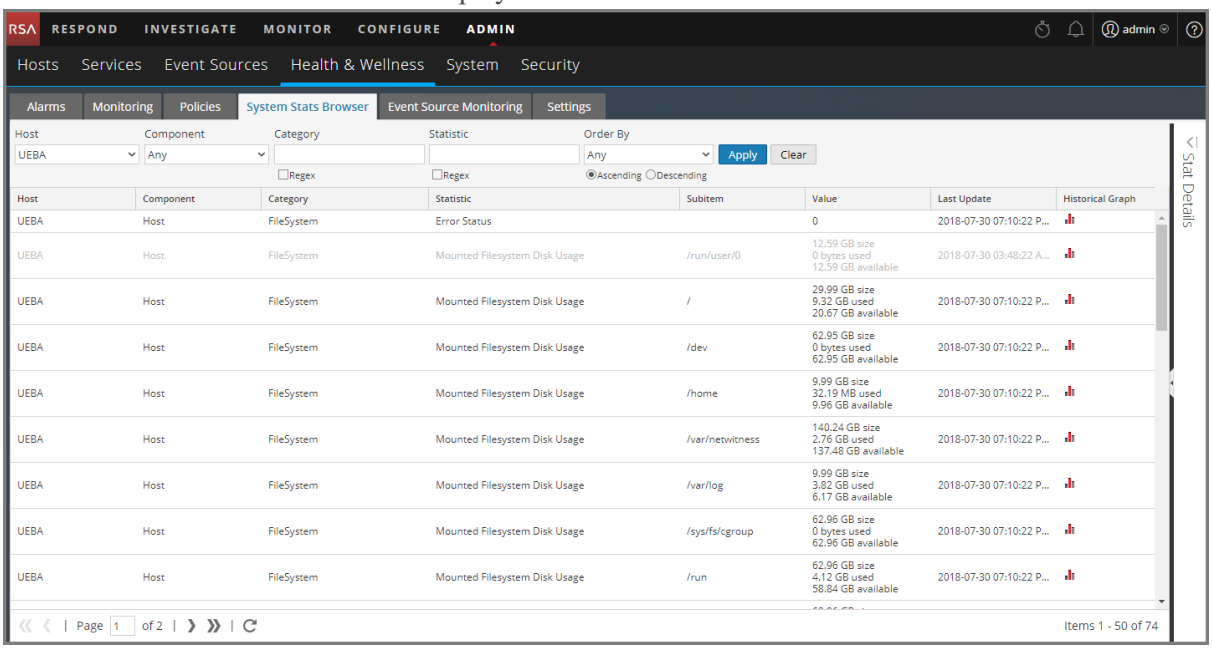
If these critical metrics are reported as "0", it may indicate a system malfunction.

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

1. Log in to NetWitness Platform and 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**.



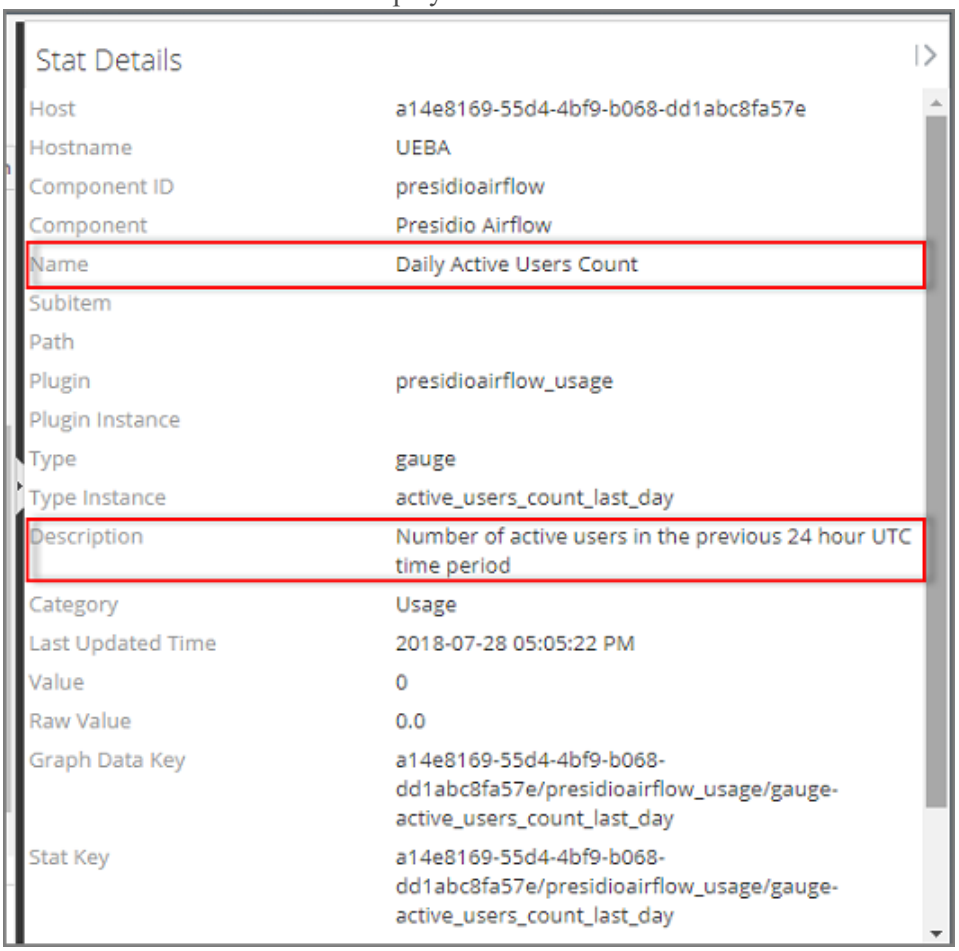
Results for NetWitness UEBA are displayed.



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

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

Details about the statistic are displayed.



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

For more information about Health & Wellness and the System Stats Browser tab, see "Monitor System Statistics" in the *System Maintenance Guide*. Go to the Master Table of Contents to find all RSA NetWitness Platform 11.x documents.

Monitor Health and Wellness of UEBA

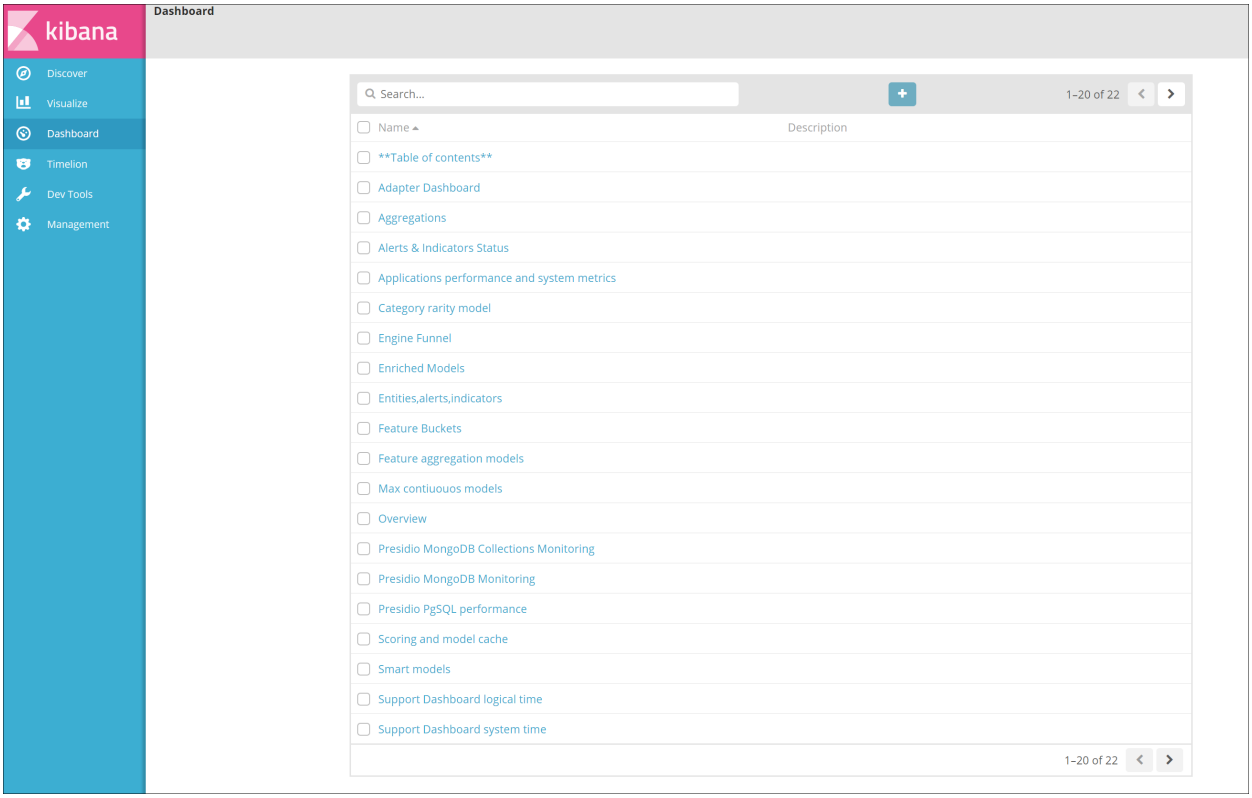
You can view the status of UEBA host in the Investigate > **ENTITIES** > **Overview** tab.

The UEBA system should generate at least 1 alert weekly. If the system stops generating the alerts for a period of 7 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 Platform: Kibana and Airflow.

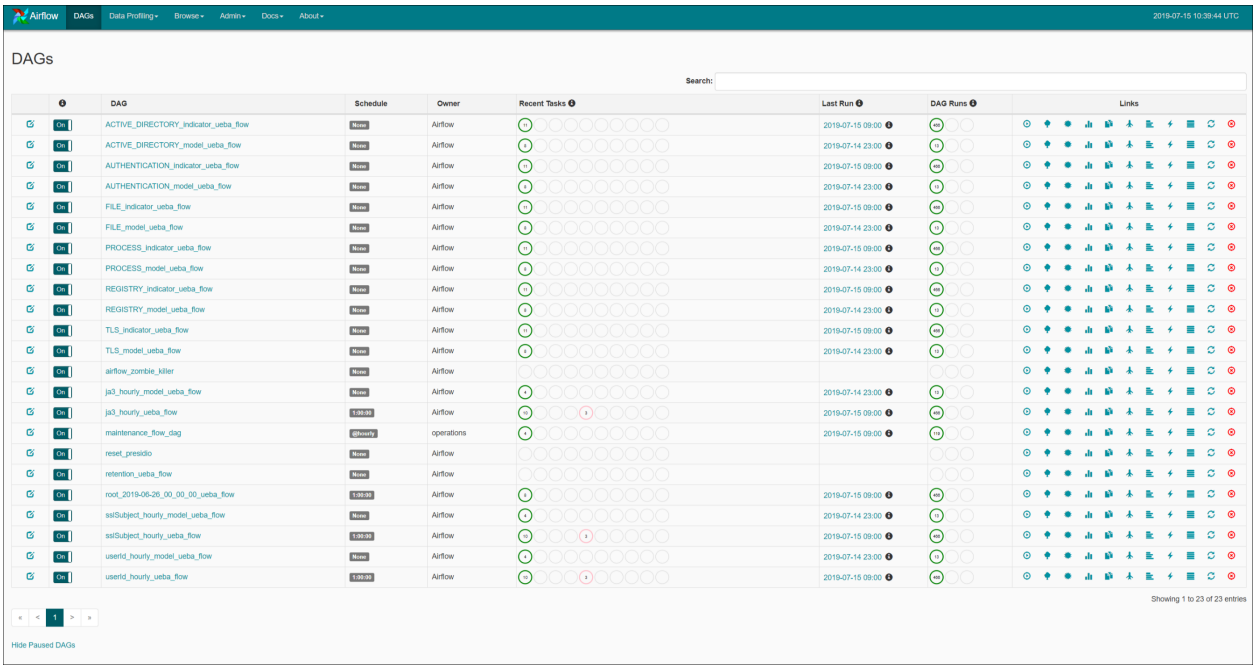
Access Kibana

To access kibana, go to *https://<UEBA_host>/kibana/app/kibana#/*, and enter user name and password. The Dashboard view is displayed.



Access Airflow

To access Airflow, go to *https://<UEBA_host>/admin/*, and enter user name and password. 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:

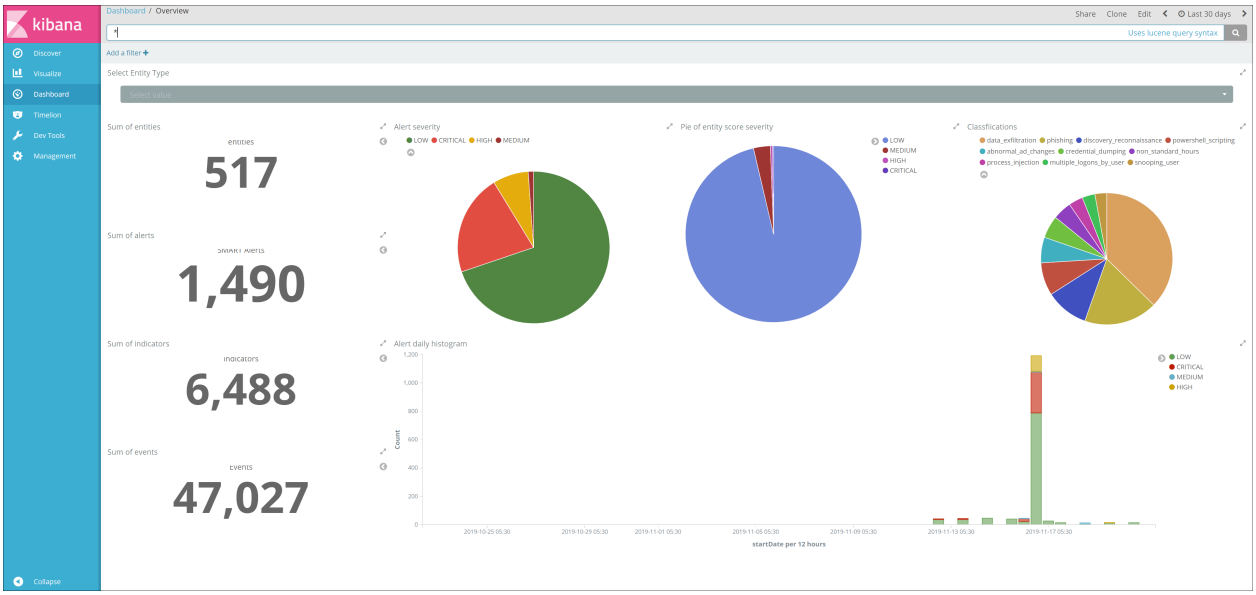
Overview Dashboard

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

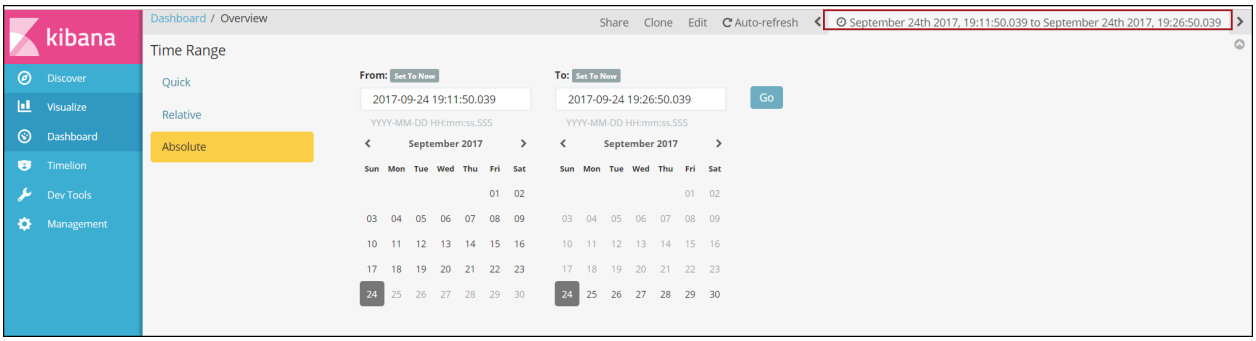
- The alerts type that are generated, and the alert severity distribution with the severity types (Low, Medium, High, Critical)
- Total number of active entities and how many alerts are generated for those entities
- The number of indicators and events processed
- The pie chart for entity score severity 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. Log into 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.



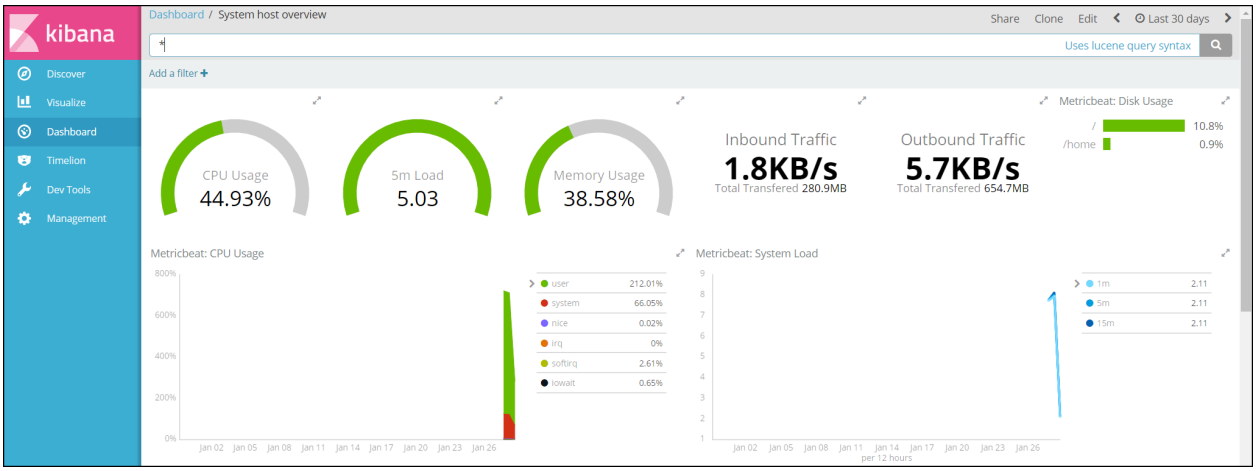
System Host overview

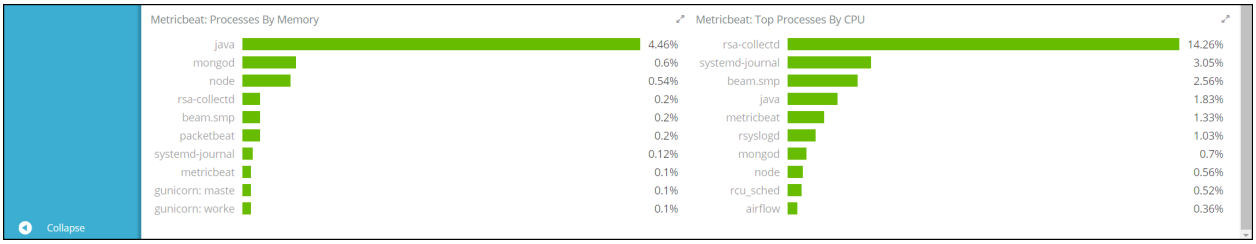
The System Host overview dashboard monitors the performance and health of UEBA host such as:

- 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 in 4 wall clock time. Once the UEBA server is online the resource utilization reduces.

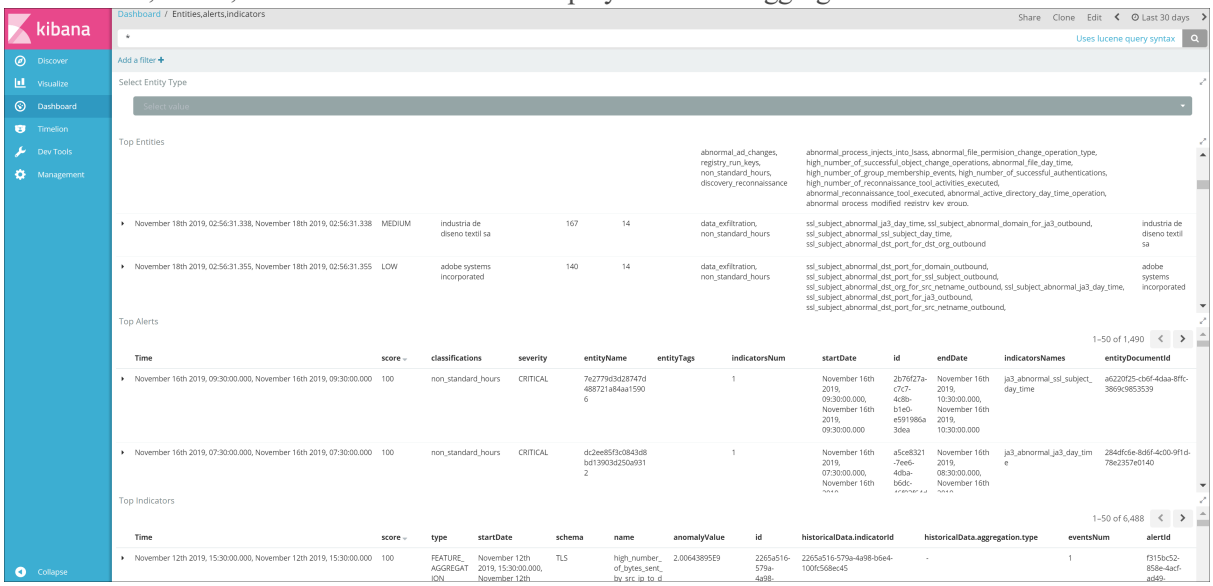
Adapter Dashboard

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

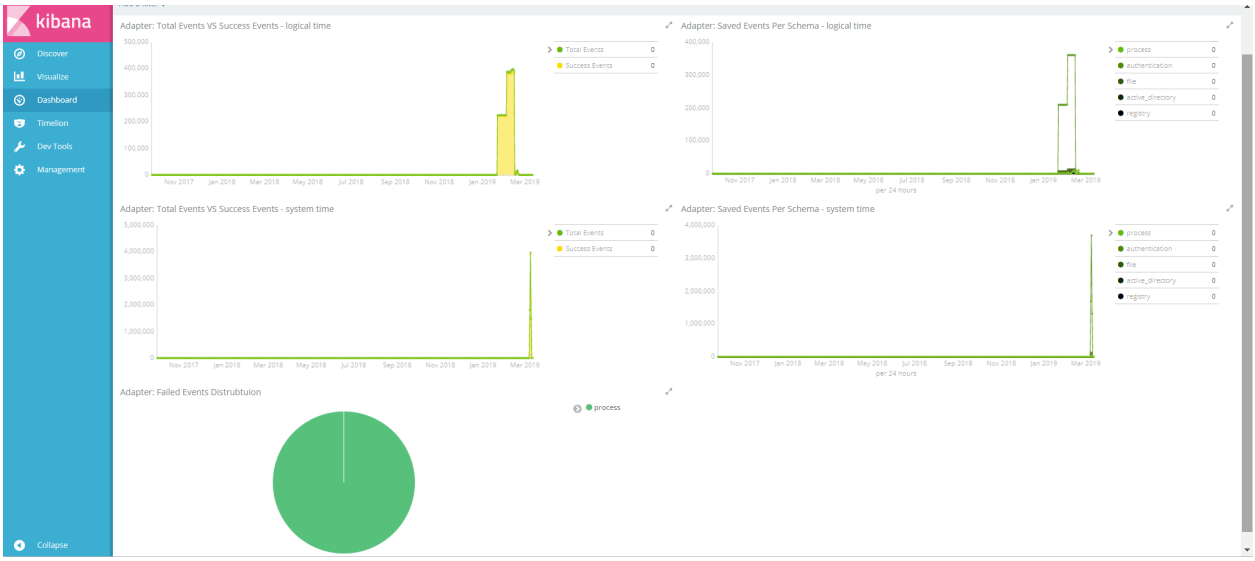
1. Log into Kibana, click **Dashboards** > **Entities, alerts, indicators**.
   The Entities, alerts, indicators Dashboard is displayed with an aggregate data for all entities.



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. Log into 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

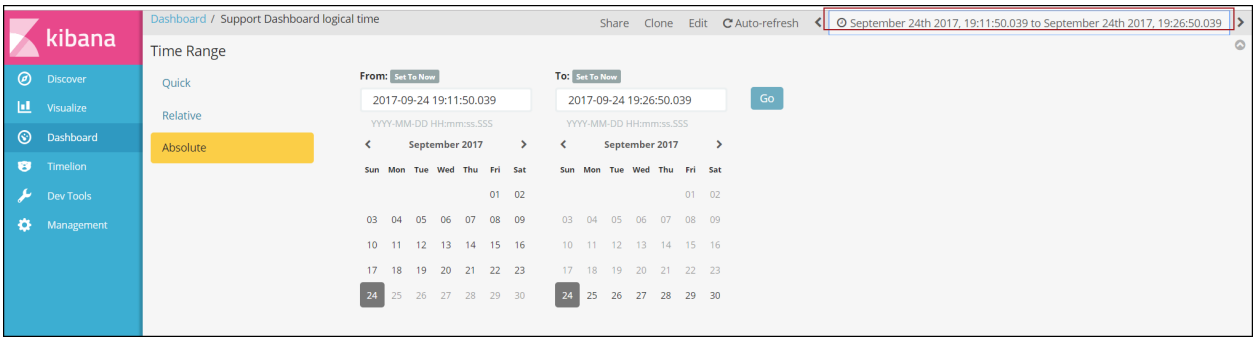
The **Support Dashboard Logical Time** provides the capability to detect the events processed time which is different form the system time such as:

- 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. Log into 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.



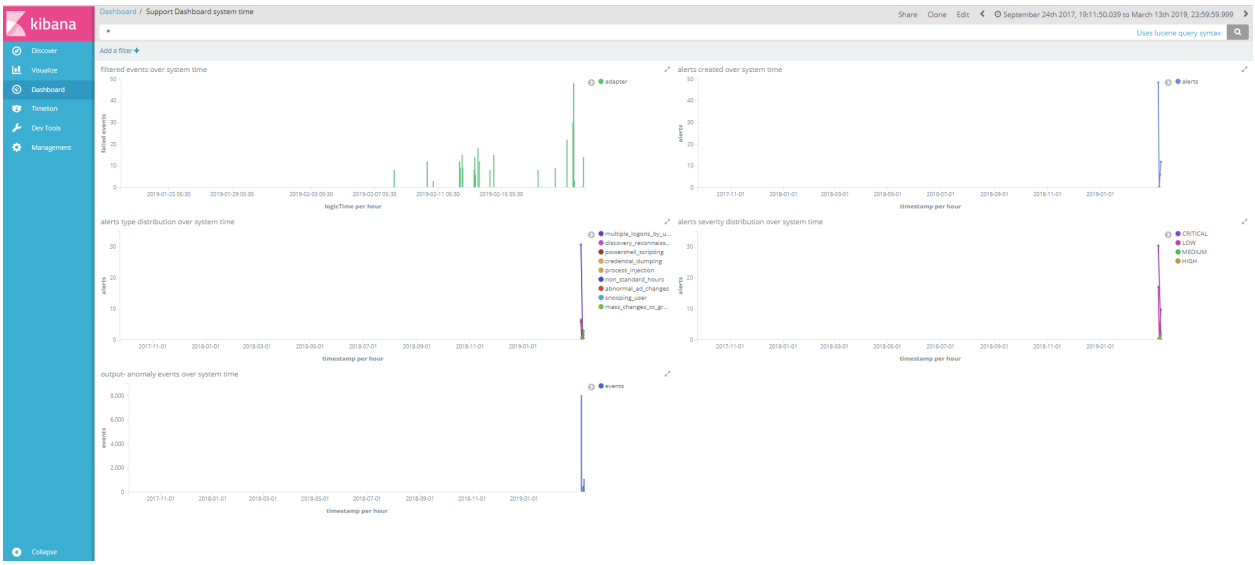
Support Dashboard System Time

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

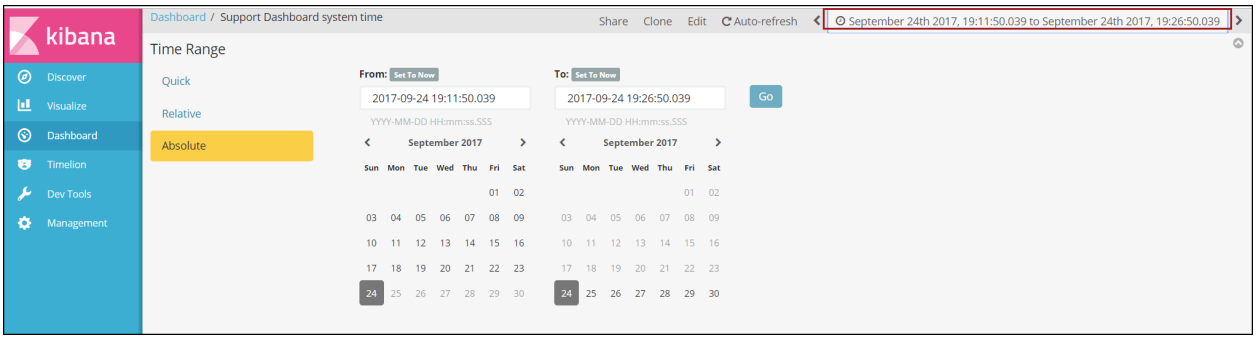
- The amount of filtered events over time per schema
- The total number of alerts generated
- The alert types distribution
- The events that are related to an alert

To access support dashboard system Time:

1. Log into Kibana, click **Dashboards** > **Support Dashboard system Time**.



2. Adjust the time range on the top right corner of the page to view the statistics.

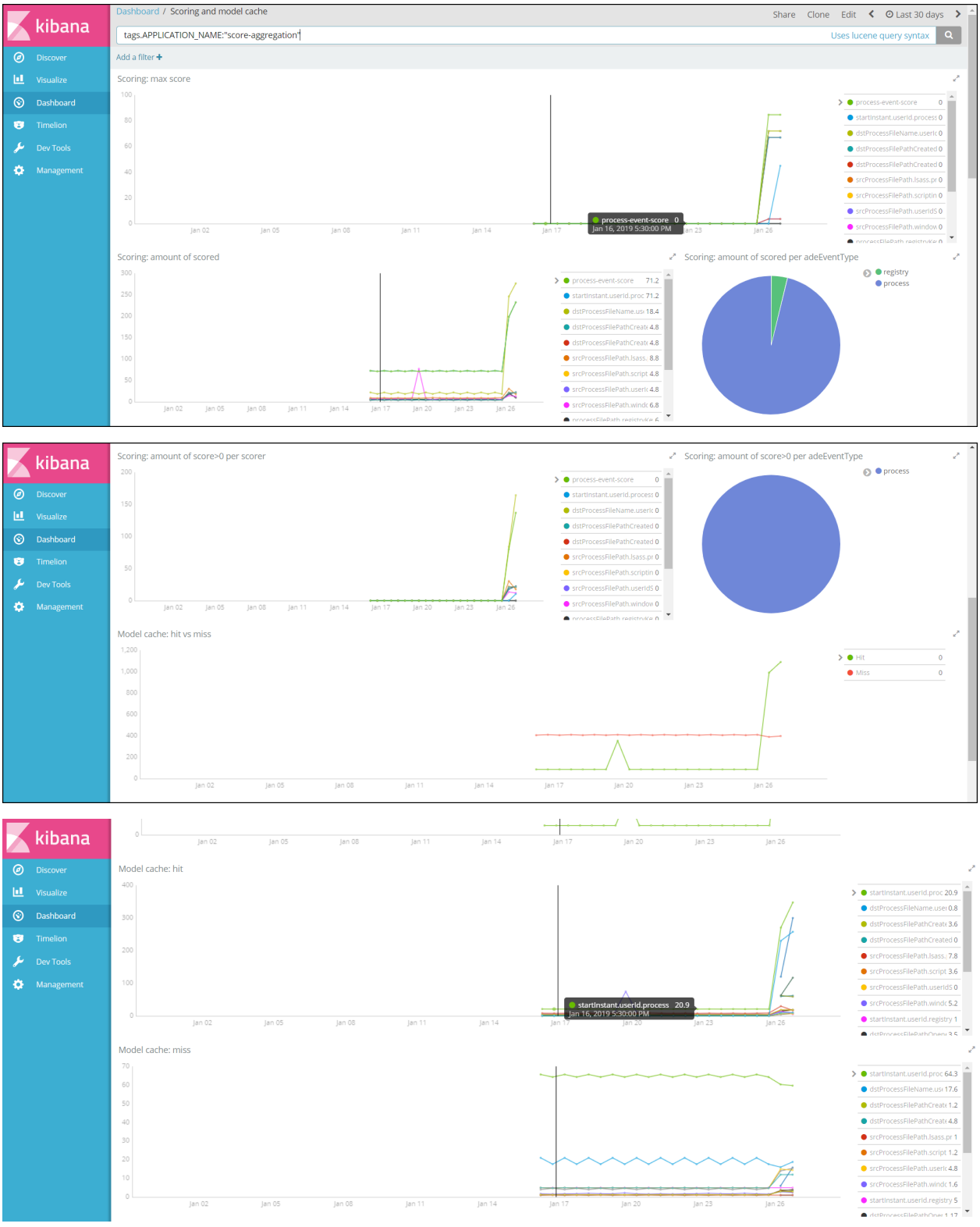


Scoring and Model Cache

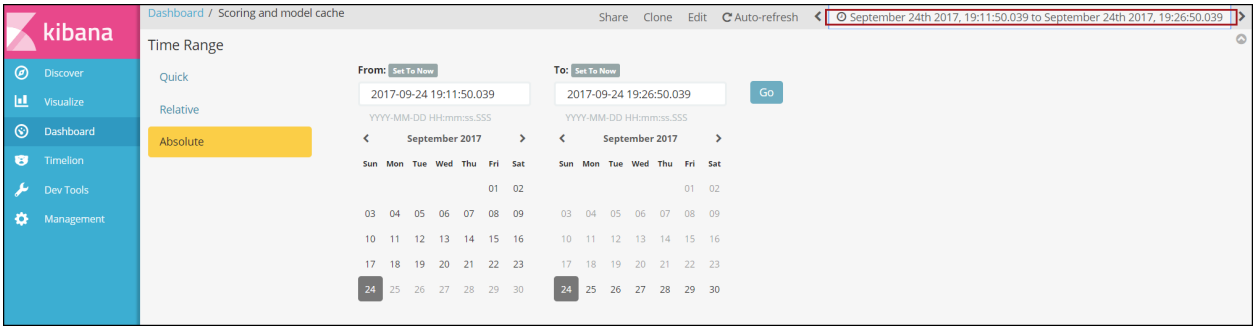
The Scoring and Model cache dashboard provides the capability to view the events being scored.

To access scoring and model cache dashboard:

1. Log into Kibana, click **Dashboards** > **Scoring and Model Cache**.
   The Scoring and model cache dashboard is displayed.


kibana
Dashboard / Scoring and model cache
Share
Clone
Edit
Last 30 days
tags.APPLICATION_NAME:"score-aggregation"
Uses lucene query syntax
Add a filter +
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Scoring: max score
process-event-score 0
Jan 16, 2019 5:30:00 PM
Scoring: amount of scored
Scoring: amount of scored per adeEventType
registry
process
Scoring: amount of score>0 per scorer
Scoring: amount of score>0 per adeEventType
Model cache: hit vs miss
Hit
Miss
Model cache: hit
startInstant.userId.process 20.9
Jan 16, 2019 5:30:00 PM
Model cache: miss

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 the 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:

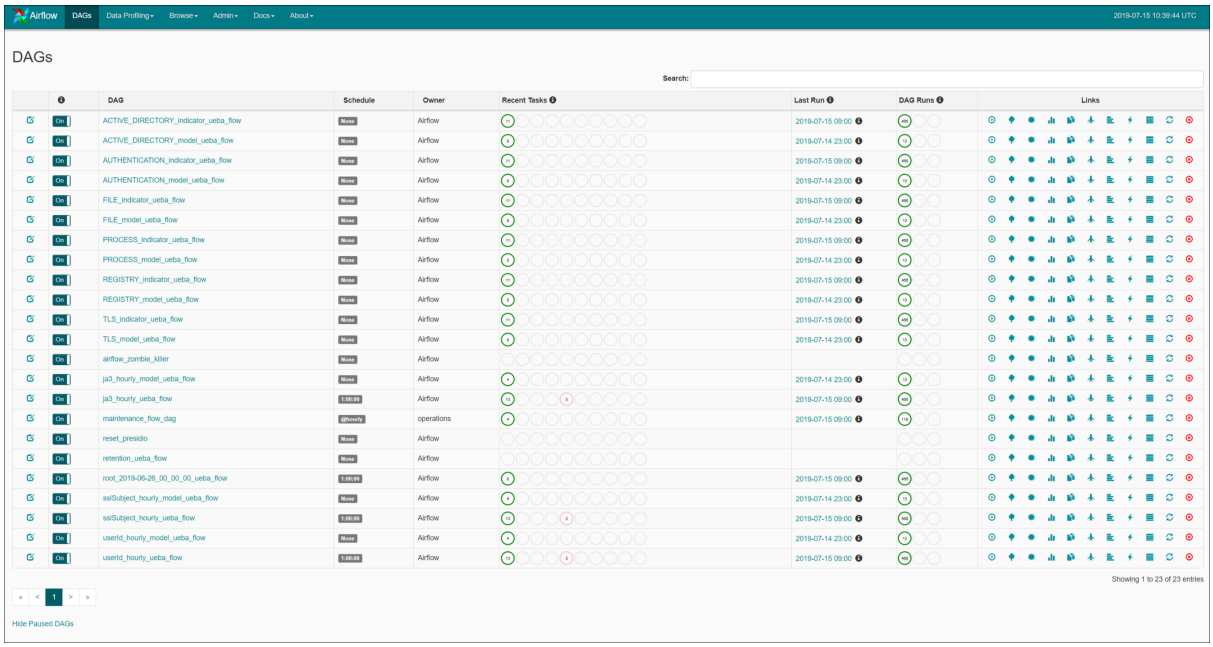
- Indicator DAG which is responsible to read events from broker and score the events based on the models.
- Model DAG which is responsible in building the models.

You can monitor the scheduled task by seeing how many tasks are successful, failed, or currently running. See the detailed information about the tasks and the logs.

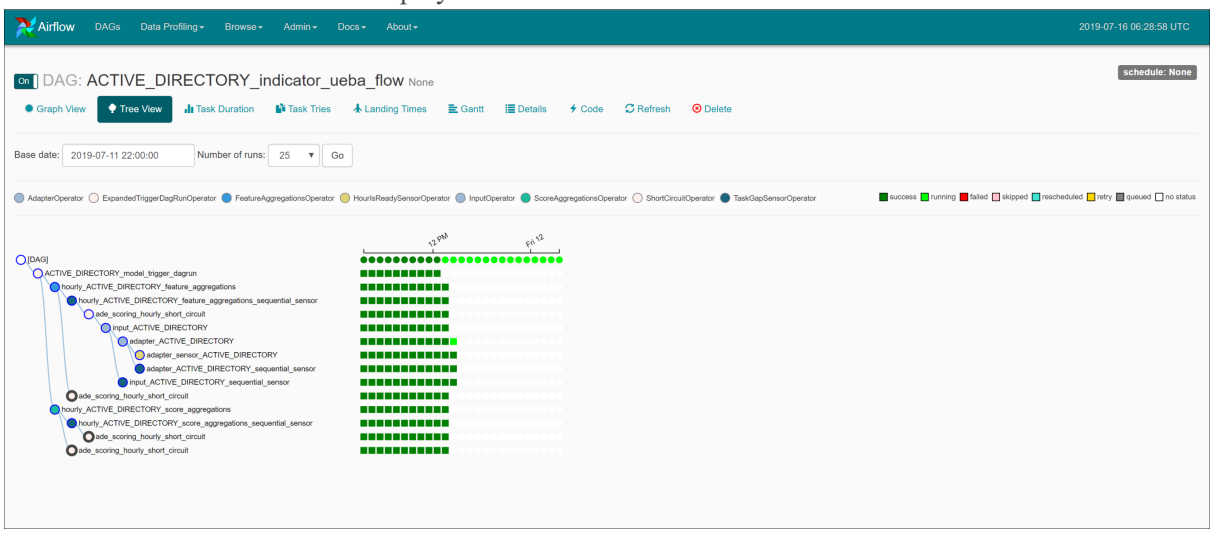
There are several DAGs and each DAG is a workflow.

To monitor the UEBA service tasks, perform the following:

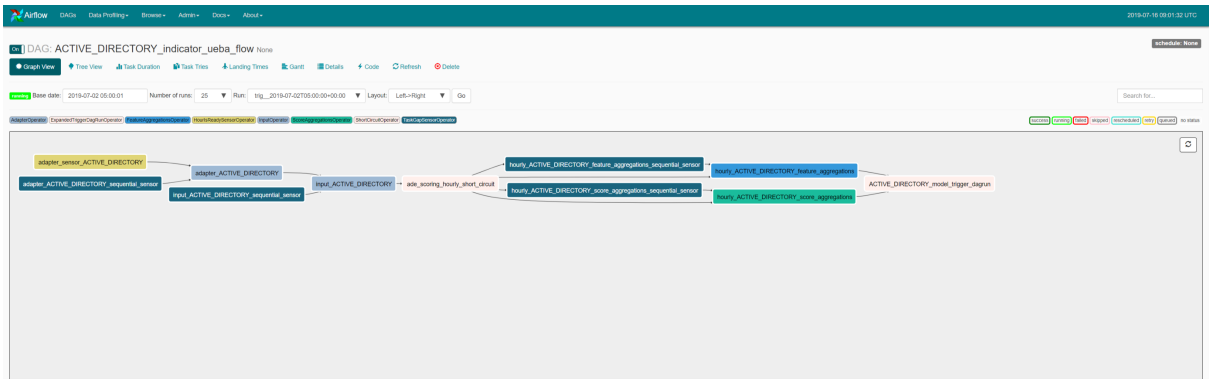
1. Log into **Airflow**.
   The DAGs view is displayed.



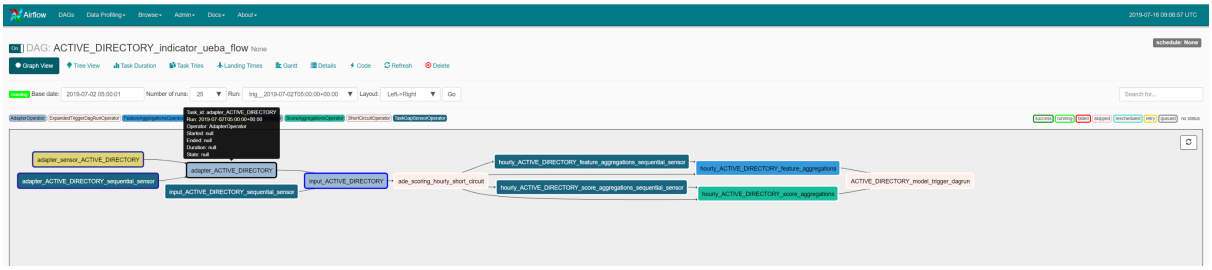
2. In the **DAG Runs** section, see the status of the tasks. For example, how many tasks are successful, failed or currently running.
3. To view the different tasks associated with the DAG, click **Tree view**.
   The Tree view of the DAG is displayed.



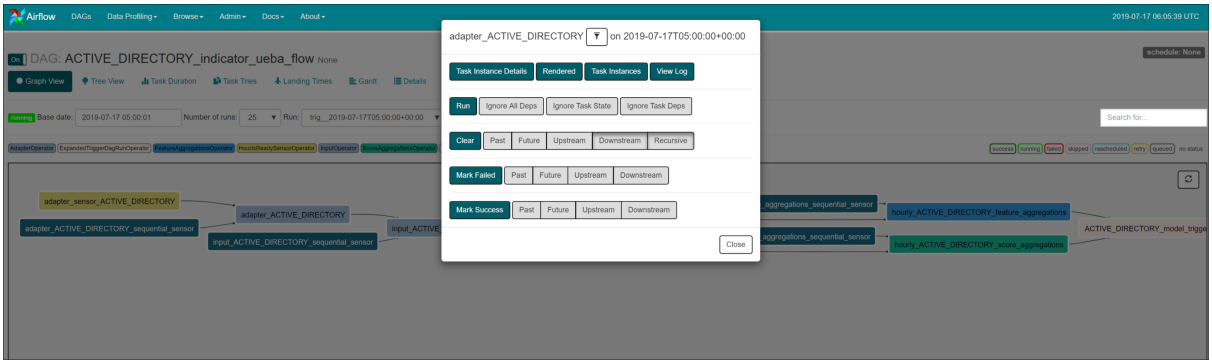
4. To view the DAG's dependencies and the current status of a specific task, in the DAG, click **Graph view**.



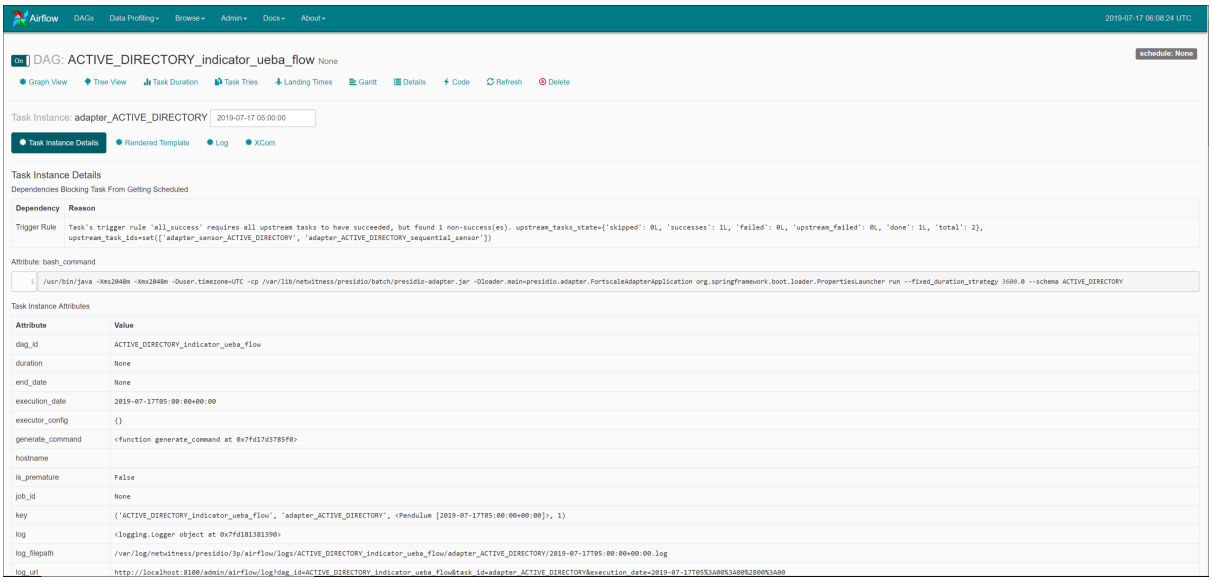
In the **Graph** view hoverover the task to see the status of the specific task.



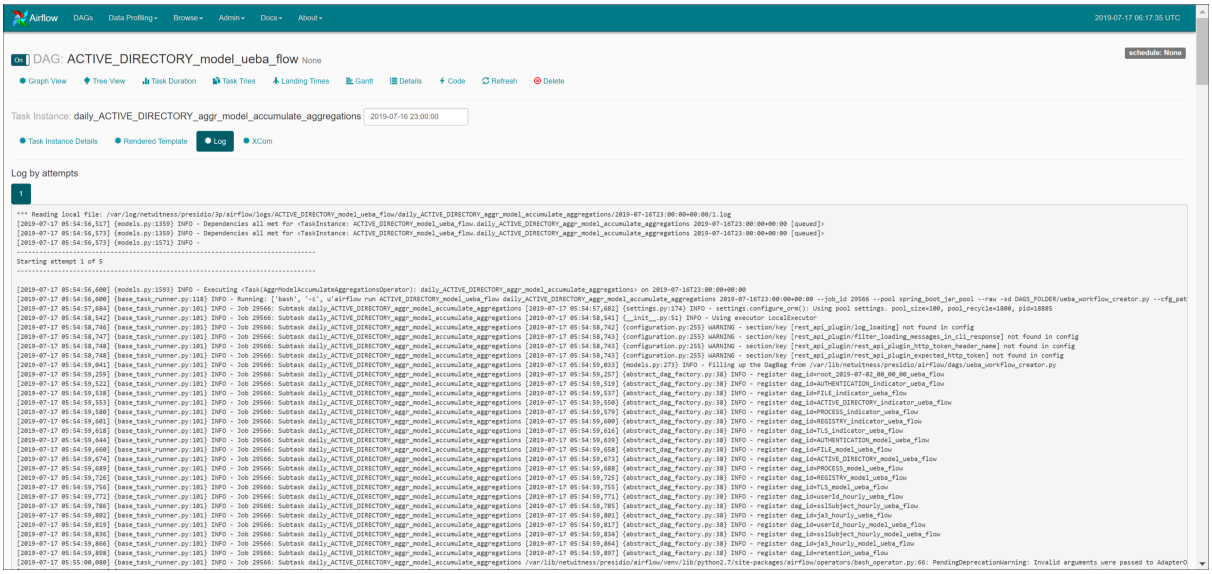
For detailed information about the specific task, click **Task** and click **Task Instance Details.**



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, else the process will stop. For more information see, Troubleshooting UEBA.

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

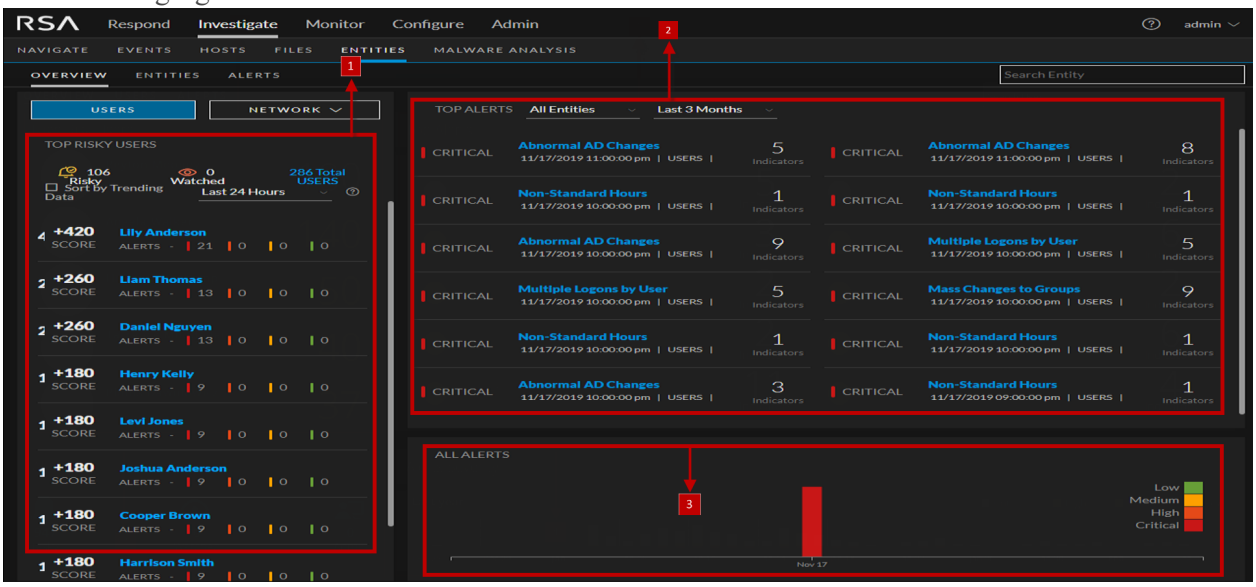
*You can complete the tasks here.

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.



To access this view, go to **Investigate** >**OVERVIEW**.

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 user or network entity 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.

Name	Description
Total Users	All user or network entities in the network.
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, and 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: 

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

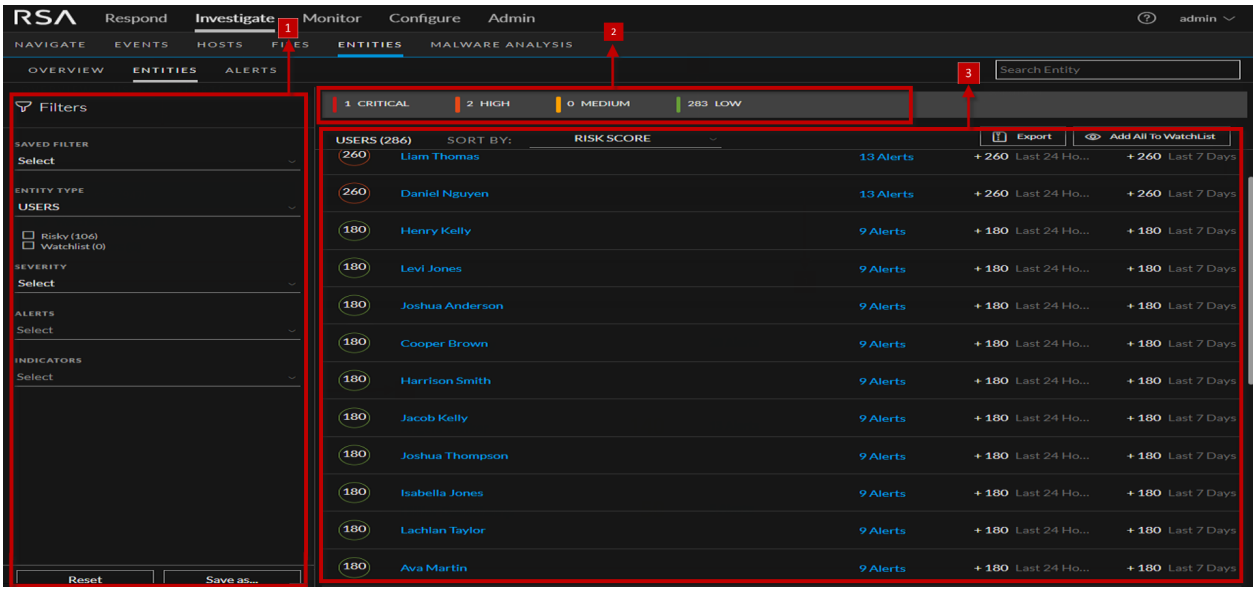
*You can complete the tasks here.

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.



To access this view:

1. Go to **Investigate** >**ENTITIES**.

   The Overview tab is displayed.

2. Click **ENTITIES**.

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.

Filter Type	Description
Severity	Severity type such as critical, high, medium and low.
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 the 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

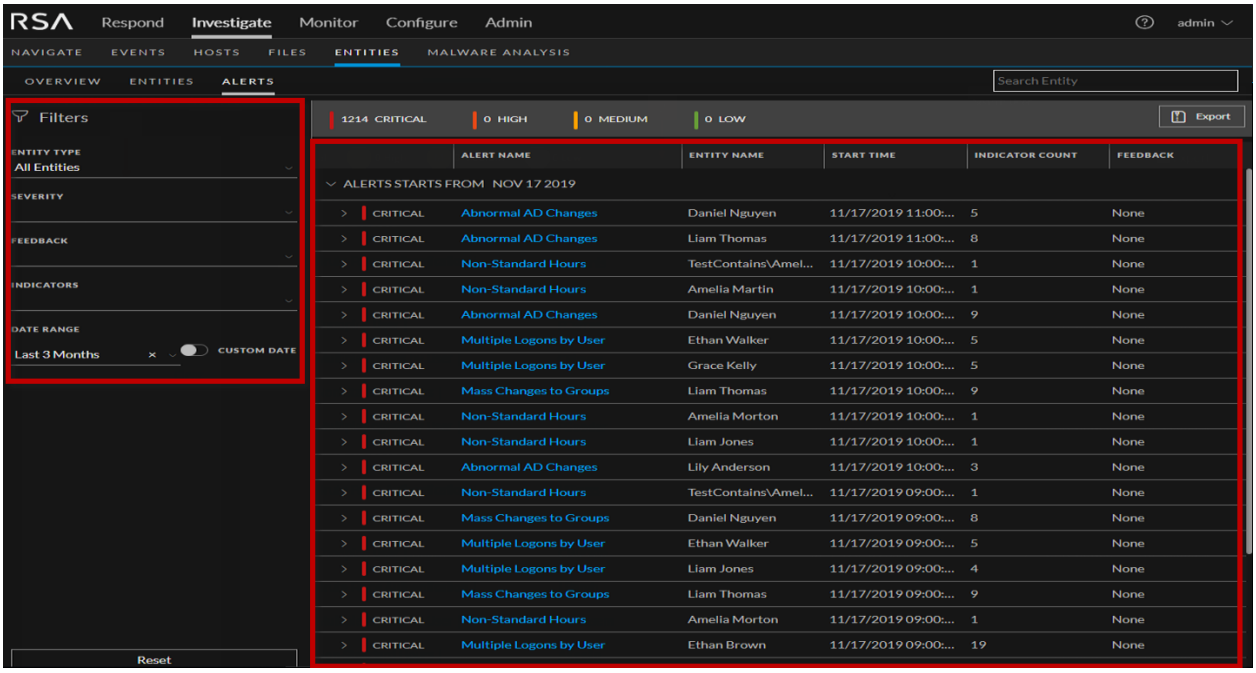
User Role	I want to ...	Documentation
UEBA Analyst	Sort alerts to focus my investigation*.	Filter Alerts
UEBA Analyst	Investigate incidents based on threat indicators*.	Investigate Events
UEBA Analyst	Share alert data in spreadsheet format.	Manage Top Alerts

*You can complete the tasks here.

Related Topics

- Investigate Top Alerts
- Filter Alerts
- Investigate Events
- Manage Top Alerts

Quick Look



To access this view:

1. Go to **Investigate** >**ENTITIES**.

   The Overview tab is displayed.

2. Click **ALERTS**.

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 has been 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:

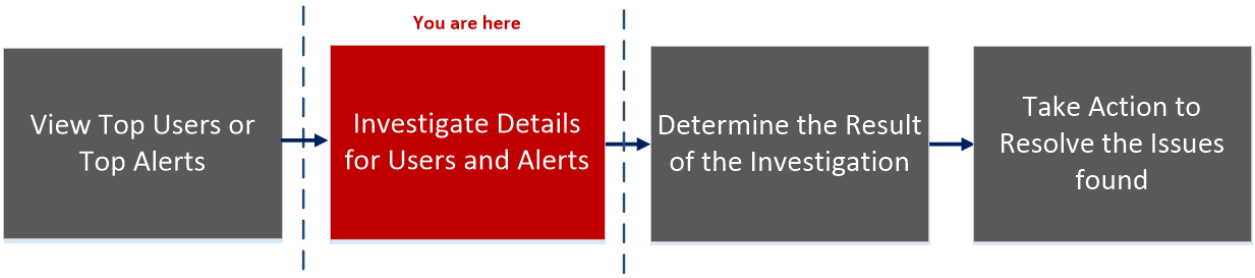
- Indicator Name – The name of each unique indicator that is associated with the alert
- Anomaly Value – The indicator's value, representing the deviation amount or value as it differs from the user's normal behavior
- Data Source – The type of data where the indicator was found
- Start Time – The date 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 Profile View

The **User Profile** view provides detailed information about all the 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

User Role	I want to ...	Documentation
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
UEBA Analyst	Investigate threat indicators.	Investigate Events

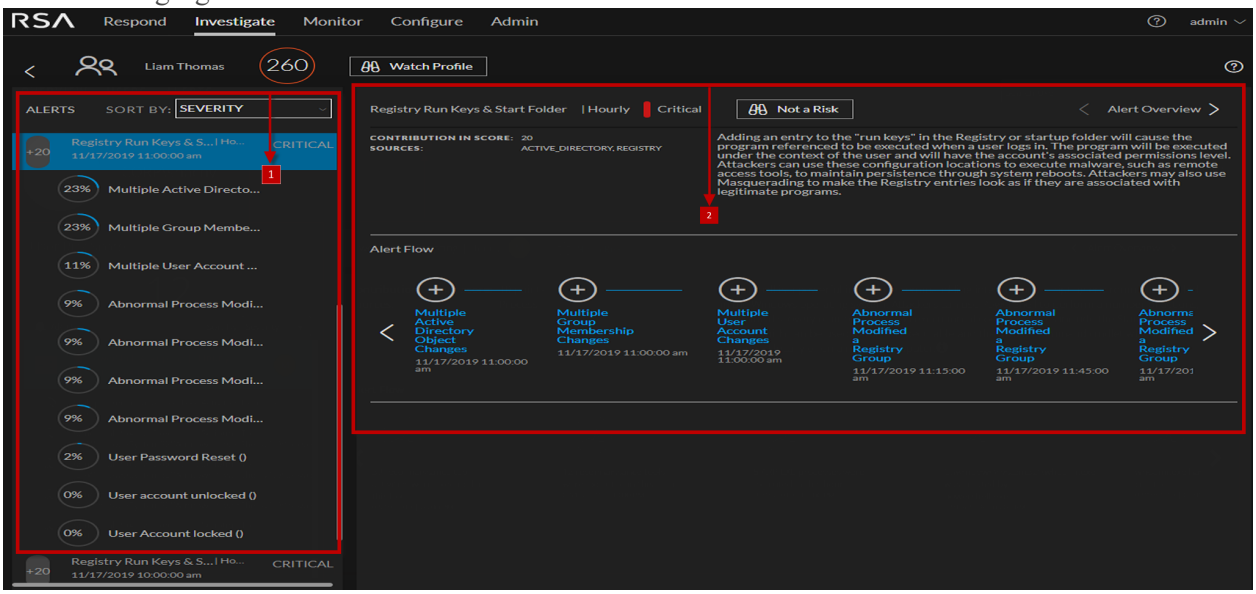
*You can complete the tasks here.

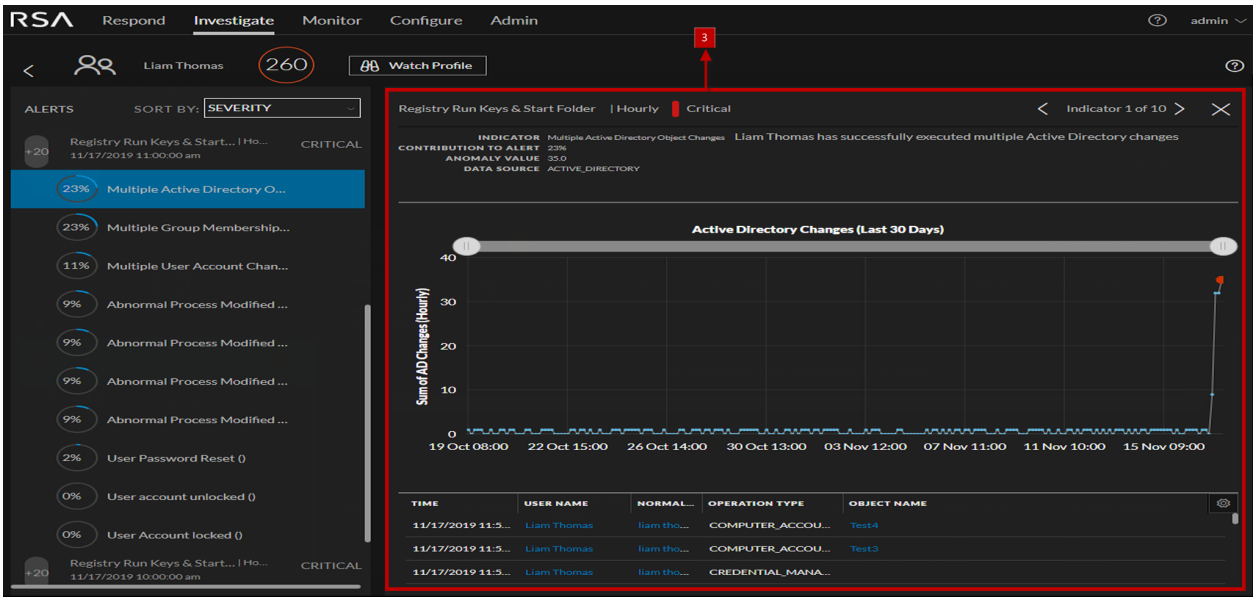
Related Topics

- 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 User Profile view.




RSA
Respond
Investigate
Monitor
Configure
Admin
admin
3
Liam Thomas
260
Watch Profile
ALERTS
SORT BY: SEVERITY
Registry Run Keys & Start... | Ho...
11/17/2019 11:00:00 am
CRITICAL
+20
23% Multiple Active Directory O...
23% Multiple Group Membership...
11% Multiple User Account Chan...
9% Abnormal Process Modified ...
9% Abnormal Process Modified ...
9% Abnormal Process Modified ...
9% Abnormal Process Modified ...
2% User Password Reset ()
0% User account unlocked ()
0% User Account locked ()
Registry Run Keys & Start... | Ho...
11/17/2019 10:00:00 am
CRITICAL
+20
Registry Run Keys & Start Folder | Hourly Critical
Indicator 1 of 10
INDICATOR Multiple Active Directory Object Changes
CONTRIBUTION TO ALERT 23%
ANOMALY VALUE 35.0
DATA SOURCE ACTIVE_DIRECTORY
Liam Thomas has successfully executed multiple Active Directory changes
Active Directory Changes (Last 30 Days)
Sum of AD Changes (Hourly)
40
30
20
10
0
19 Oct 08:00
22 Oct 15:00
26 Oct 14:00
30 Oct 13:00
03 Nov 12:00
07 Nov 11:00
11 Nov 10:00
15 Nov 09:00
TIME
USER NAME
NORMAL...
OPERATION TYPE
OBJECT NAME
11/17/2019 11:5...
Liam Thomas
liam tho...
COMPUTER_ACCOU...
Test4
11/17/2019 11:5...
Liam Thomas
liam tho...
COMPUTER_ACCOU...
Test3
11/17/2019 11:5...
Liam Thomas
liam tho...
CREDENTIAL_MANA...

To access this view:

1. Go to **Investigate** >**ENTITIES**. Do any of the following:
   a. In the **OVERVIEW** tab, under **TOP RISKY USERS** panel, click on the username.
   b. In the **ENTITIES** tab, click on the username.
   c. In the **ALERTS** tab, click on the alert name.

The Users Profile consist of the following panels:

1 User Risk Score panel
2 Alerts Flow panel
3 Indicator 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 following information is displayed: • The alert names • The severity level icon • The start date and time for the alert • The timeframe of the alert (Hourly) • The risk score of the alert (+20) • A 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)

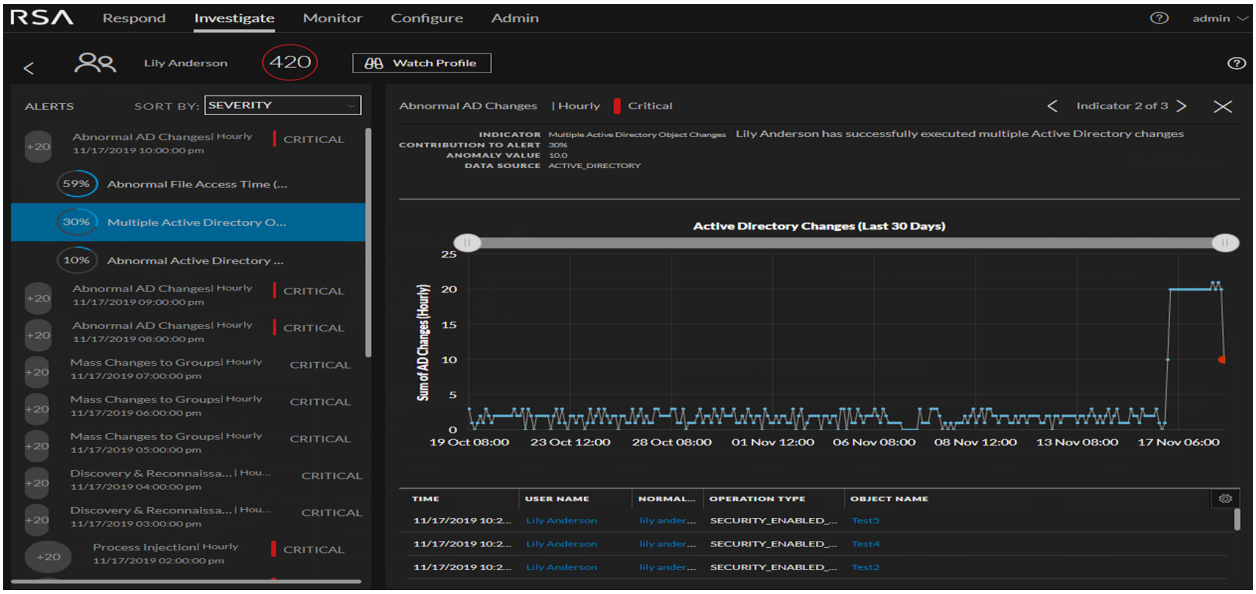
Name	Description
Sources	The data sources for the alert. (For example, Active Directory)
Tamerlane graph	The timeline of events that are related to the formation of the alert.

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.

Event Name	Description
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.
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.

Event Name	Description
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.

Event Name	Description
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	The number of the destination ASN.
JA3S	The JA3S hash value.
Destination Netname	The name of the destination netname.
Number of Bytes Received	The number of bytes received.

Troubleshooting UEBA

This section provides information about possible issues when using NetWitness UEBA.

Scaling Limitation Issue

When installed on a Virtual Machine, UEBA can process up to 20 million network events per day. Based on this limitation, you may encounter the following issues.

Issue	How to determine the scale of network events currently available, to know if it exceeds the UEBA limitation.
Solution	To know the network data limit, perform the following : • Run the query on the Broker or Concentrator that connects to UEBA using NetWitness UI: `service=443 && direction='outbound' && analysis.service!='quic' && ip.src exists && ip.dst exists && tcp.srcport!=443` Calculate the total number of events for the selected days (including weekdays with standard workload). If the average is above 20 million per day then it indicates that UEBA's supported scale is exceeded.

Issue	Can UEBA for Packets be used if UEBA's supported scale is exceeded?
Solution	You must create or choose a Broker that is connected to a subset of Concentrators that does not exceed the supported limit. To know the network data limit, perform the following : • Run the query on the Concentrator that connects to UEBA using NetWitness UI: `service=443 && direction='outbound' && analysis.service!='quic' && ip.src exists && ip.dst exists && tcp.srcport!=443` Calculate the total number of events for the selected days (including weekdays with standard workload). If the average is above 20 million per day then it indicates that UEBA's supported scale is exceeded.

Note: The Broker must query all the available and needed data needed such as logs, endpoint and network (packets).

Note: UEBA packets models are based on the whole environment. Hence, make sure that the data parsed from the subset of Concentrators is consistent.

UEBA policy Issue

Issue	After you create a rule under UEBA policy, duplicate values are displayed in the Statistics drop-down.

Solution	To remove the duplicate values perform the following:
	1. Log in to MongoDB using following command:mongo admin -u deploy_ admin -p {Enter the password}
	2. Run the following command on MongoDB
	`use sms;`
	`db.getCollection('sms_statdefinition').find({componentId :"presidioairflow"})`
	`db.getCollection('sms_statdefinition').deleteMany ({componentId :"presidioairflow"})`

Troubleshoot using Kibana

Issue	After you deploy NetWitness UEBA, the connection between the NetWitness Platform and NetWitness UEBA is successful but there are very few or no events in the **Investigate** > **Users** tab. 1. Log in to **Kibana**. 2. Go to **Table of Content** > **Dashboards** > **Adapter Dashboard**. 3. Adjust the **Time Range** on the top right corner of the page and review the following: • If the new events are flowing. • In the **Saved Events Per Schema** graph, see the number of successful events per schema per hour. • In the **Total Events vs. Success Events** graph, see the total number of events and number of successful events. The number of successful events should be more every hour. For example, in an environment with 1000 users or more, there should be thousands of authentication and file access events and more than 10 Active Directory events. If there are very few events, there is likely an issue with Windows auditing.
Solution	You must identify the missing events and reconfigure the Windows auditing. 1. Log into **NetWitness Platform** and go to **INVESTIGATE** > **Navigate**. 2. Filter by **devide.type= device.type "winevent_snare"** or **"winevent_nic"**. 3. Review the events using **reference.id** meta key to identify the missing events. 4. Reconfigure the Windows auditing. For more information, see **NetWitness UEBA Windows Audit Policy** topic.

Issue	The historical load is complete and the events are coming from Adapter dashboard but no alerts are displayed in the **Investigate** > **Users** tab.
Solution	1. Go to **Kibana** > **Table of content** > **Scoring and model cache**. 2. Adjust the **Time Range** on the top right corner of the page, and see if the events are being scored.

Issue	The historical load is complete but no alerts are displayed in the **Investigate** > **Users** tab.
Solution	1. Go to **Kibana** > **Dashboard** > **Overview**. 2. Adjust the **Time Range** on the top right corner of the page, to see how many users are analyzed and if any anomalies are found.

Troubleshoot using Airflow

Issue	After you start running the UEBA it is not possible to remove a data source during the run process else the process will stop.
Solution	You must either continue the process till it completes or remove the required data source from UEBA and rerun the process.

Issue	After you deploy UEBA and if there are no events displayed in the **Kibana** > **Table of content** > **Adapter** dashboard and the Airflow already processed the hours but there are no events. This is due to some communication issue.
Solution	You must check the logs and resolve the issue. 1. Login to **Airflow**. 2. Go to **Admin** > **REST API Plugin**. 3. In the **Failed Tasks Logs**, click **execute**. A zip file is downloaded. 4. Unzip the file and open the log file to view and resolve the error. 5. In the **DAGs** > **reset_presidio**, click **Trigger Dag**. This deletes all the data and compute all the alert from the beginning. **Note:** During initial installation, if the hours are processed successfully but there is no events, you must click reset_presidio after fixing the data in the Broker. Do not reset if there are alerts.

Appendix: NetWitness UEBA Windows Audit Policy

In order to achieve the 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, refer to 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, as well as 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

Revision History

Revision	Date	Description	Author
0.1	12-Mar-19	Final Draft	IDD