RSA NETWITNESS® PLATFORM

NetWitness Investigate Quick Start 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

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

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

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

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.

April 2020

What Is NetWitness® Investigate?

NetWitness Platform audits and monitors all traffic on a network. One type of service--a Decoder--ingests, parses, and stores the packets, logs, and endpoint data traversing the network. The configured parsers and feeds on the Decoder create *metadata* that analysts can use to investigate the ingested logs and packets. Another type of service, called a Concentrator, indexes and stores the metadata. NetWitness Investigate provides the data analysis capabilities in RSA NetWitness® Platform, so that analysts can analyze packet, log, and endpoint data, and identify possible internal or external threats to security and the IP infrastructure.

About This Guide

This guide provides end-to-end guidelines for all members of the SOC team to configure NetWitness Investigate and to investigate log and network events. End-to-end guidelines for investigating endpoints and user entity behavior using NetWitness Investigate are provided in separate documents:

- *NetWitness Endpoint Quick Start Guide*
- *NetWitness UEBA Quick Start Guide*

RSA NetWitness Platform 11.4 Documentation in RSA Link

NetWitness Platform product documentation is organized along functional lines. If you are looking for a specific guide or version, go to the Version 11.x Master Table of Contents.

Use these links to view the RSA NetWitness Platform 11.4 documentation. Both links provide the same documentation, in these two formats:

- HTML Guides include the latest information for currently supported 11.x versions: RSA NetWitness Platform 11.x Documentation.
- A tasks map links to relevant Version 11.4 topics and guides: RSA NetWitness Platform 11.4 Product Documentation
- PDF Guides provide the information for a specific version: RSA NetWitness Platform 11.4 PDFs.

Use these links to access documentation that is not related to a particular version of the software:

- Hardware setup guides: https://community.rsa.com/community/products/netwitness/hardware-setup-guides
- Documentation for RSA Content such as feeds, parsers, application rules, and reports: https://community.rsa.com/community/products/netwitness/rsa-content.

Getting Started

The following tasks can be performed in any sequence and are for the entire SOC team.

Description	References
	
View information about product updates, improvements, and known issues	*Release Notes for RSA NetWitness Platform 11.4*
Understand how NetWitness Investigate works	"How NetWitness Investigate Works" in the *NetWitness Investigate User Guide*

Setup, Installation, or Upgrade

No special setup, installation, or upgrade tasks are required for Investigate; it is part of NetWitness Platform for Logs and Network. However, setup is required for several components with which NetWitness Investigate works if you plan to do this type of analysis. These tasks are for the Administrator, and the SOC Manager may want to understand the setup.

Description	References
	
Install and set up the Malware Analysis (standalone or service)	Malware Analysis Configuration Guide
Install and set up NetWitness Endpoint (standalone or service)	NetWitness Endpoint Quick Start Guide
Install and set up NetWitness UEBA (standalone or service)	NetWitness UEBA Quick Start Guide

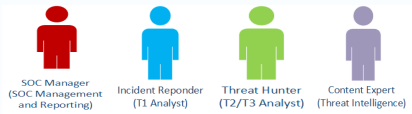
System-Level Configuration

Administrators configure system-level preferences for NetWitness Investigate.The following tasks are for the administrator, and the tasks can be performed in any sequence. SOC Managers should understand the possible configuration options.

Description	References
	
Configure role-based access control (RBAC) for analysts who will be using Investigate. These components have permissions related to investigate: investigate (Navigate view and Legacy Events view), investigate-server (Events view), Malware (Malware Analysis view), Endpoint-broker-server, and Endpoint-server.	"Role Permissions" in the System Security and User Management Guide
Configure Investigate to limit content available for different user roles (preQueries).	"Verify Query and Session Attributes per Role" in the System Security and User Management Guide
Configure default settings and limits for NetWitness Investigate on a system level.	"Configure Investigation Settings" in the System Configuration Guide

User Preference Configuration

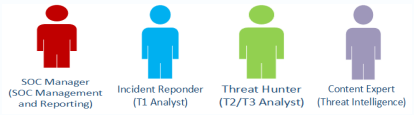
The following tasks are for Threat Hunters, Content Experts, and Incident Responders, and SOC Managers. The tasks can be performed in any sequence.

Description	References
	
Configure Navigate view and Legacy Events view preferences.	"Configure the Navigate and Legacy Events View" in the *NetWitness Investigate User Guide*
Configure Events view preferences.	"Configure the Events View" in the *NetWitness Investigate User Guide*
Configure the Malware Analysis view preferences.	"Configure Malware Analysis" in the *Malware Analysis User Guide*

Investigation

Different types of investigation may be handled by analysts with different skill levels and goals.

- Incident Responders (T1 Analysts) typically pivot to Investigate from NetWitness Respond to find detailed information about an incident so that they can respond to and remediate incidents.
- Threat Hunters (T2/T3 Analysts) typically peruse events, metadata, and raw content so that they can recommend issues for remediation and remediate issues.
- Content Experts (Threat Intelligence) typically peruse events, metadata, raw content, user and host data, and UEBA data so that they can investigate new threat intelligence, evaluate and create new feeds, and create correlation rules to flag indicators of compromise.
- SOC Managers need to understand the use cases.

Description	References
	
Learn about practical use cases	"Sample Use Cases for NetWitness Investigate" in the *NetWitness Investigate User Guide*
Investigate metadata and raw events in logs and network traffic	"Beginning an Investigation" in the *NetWitness Investigate User Guide*
Investigate possible malware	Malware Analysis User Guide
Investigate endpoints	NetWitness Endpoint User Guide
Perform user and entity behavior analysis	NetWitness UEBA User Guide

Maintenance

The administrator can perform the following tasks in any sequence.

Description	References
	
Maintain the list of queries and analyze the query patterns of other users of the NetWitness Platform system.	"Maintaining Queries Using URL Integration" in the System Maintenance Guide

Description	References
Fine tune system-level configuration settings to improve performance or limit access to data.	"Verify Query and Session Attributes per Role" in the System Security and User Management Guide "Configure Investigation Settings" in the System Configuration Guide