RSA® NETWITNESS®
Security Operations Implementation Guide

Verodin SIP

Jeffrey Carlson, RSA Partner Engineering
Last Modified: April 13th, 2017

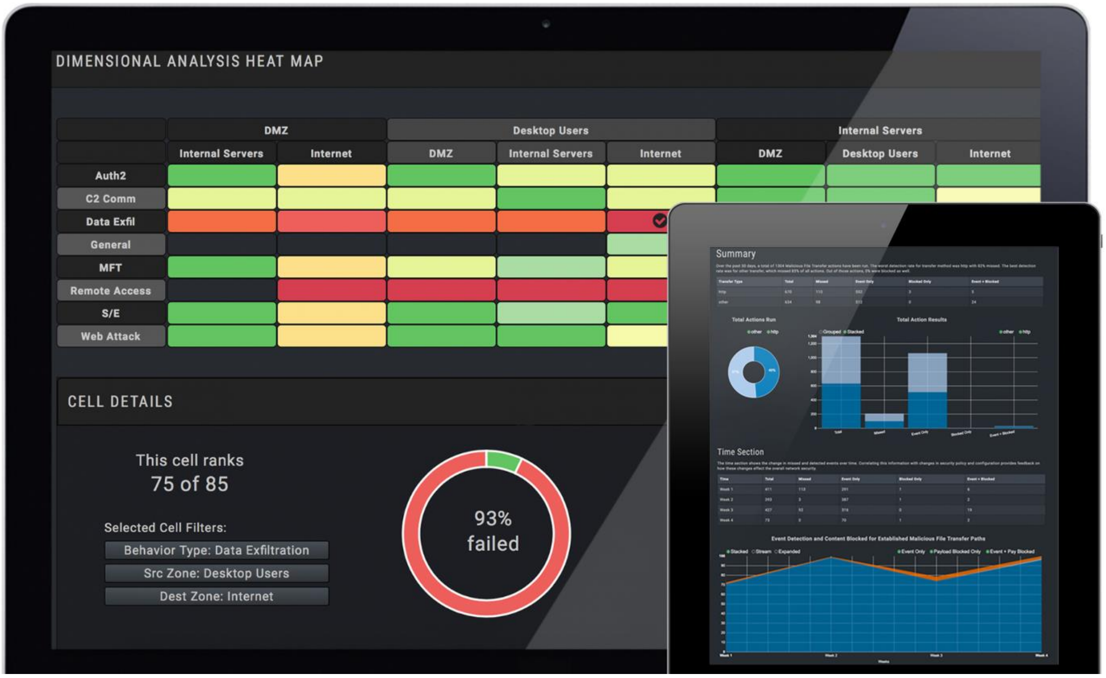
RSA READY

Solution Summary

Verodin's Instrumented Security™ platform is a foundational technology -a new approach to managing your cyber-security lifecycle. By demonstrating the impact of modern threats and malicious activities within the context of your environment, Verodin proves the effectiveness of your investments, proactively identifies configuration issues in your security stack and exposes true gaps across your people, process and technology.

Verodin provides clarity on what a threat means for you and empowers you to drive decisions and priorities with evidence-based data.

Verodin's integration with RSA NetWitness automatically extracts evidence-based data on how the layered defenses reacted, thereby proving the effectiveness of your security tools and allowing analysts to further tune or identify any gaps in the RSA NetWitness configuration.



This cell ranks
75 of 85

Selected Cell Filters:
Behavior Type: Data Exfiltration
Src Zone: Desktop Users
Dest Zone: Internet

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Verodin SIP with RSA NetWitness. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Verodin components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Verodin SIP is properly configured and secured before deploying to a production environment. For more information, please refer to the Verodin SIP documentation or website.

Verodin SIP Prerequisites

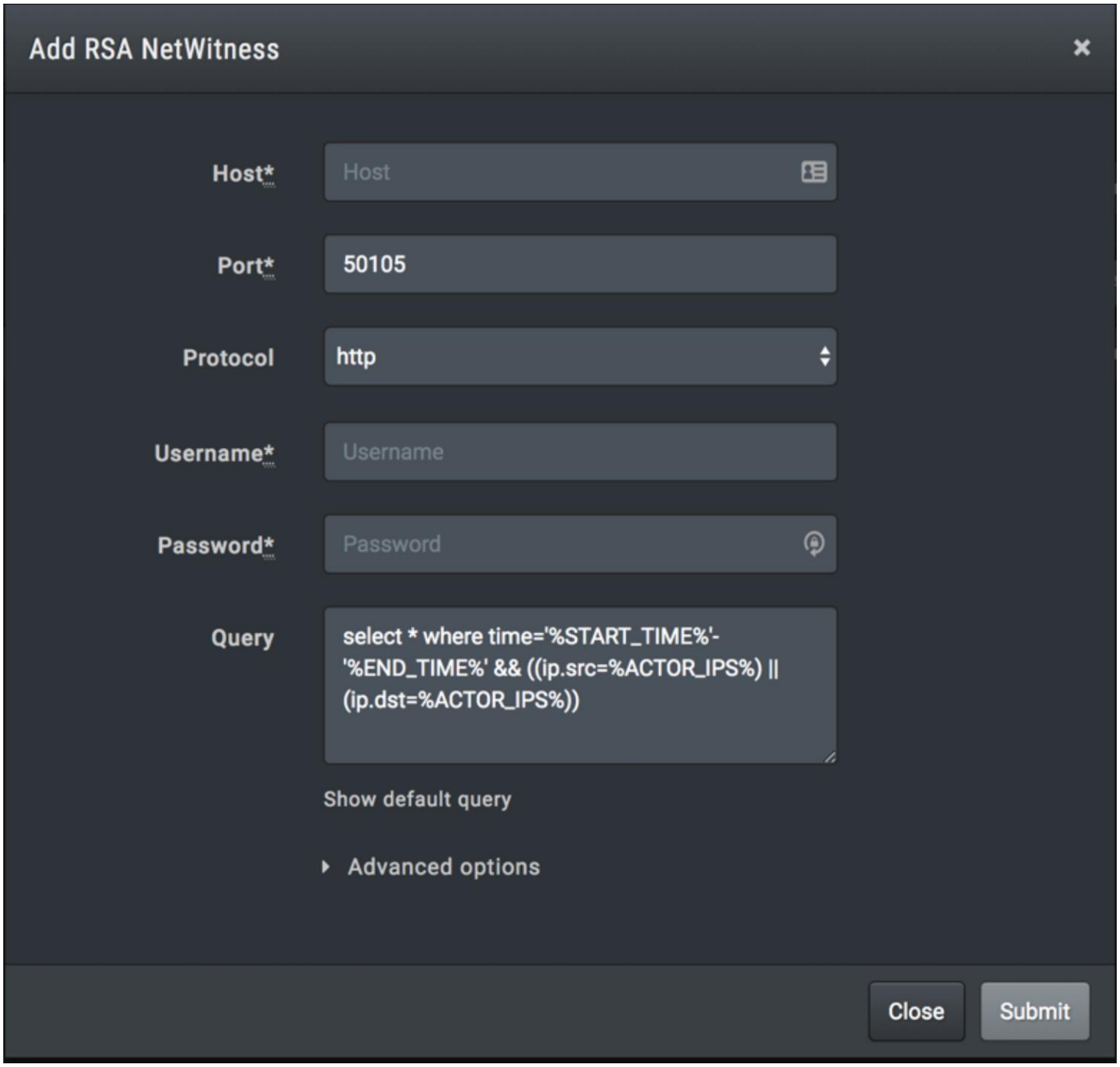
The RSA NetWitness integration has the following requirements and prerequisites:

1. Identify the IP address used to access the RSA NetWitness concentrator.
2. Identify the port for the concentrator communication (default is 50105).
3. Identify whether the protocol is HTTP or HTTPS for connections to the RSA NetWitness Concentrator port.
4. Identify or create the credentials to access the RSA NetWitness Concentrator.
5. Identify the field name mappings for the following (there could be multiples of each, depending on log sources and configuration):
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Event Start Time (timestamp)
    - Event Unique ID
    - Event Signature ID
    - Event Description
    - Event Source Host

6. Verify the Director can communicate with the RSA NetWitness Concentrator IP address on the port specified.

Verodin SIP Configuration

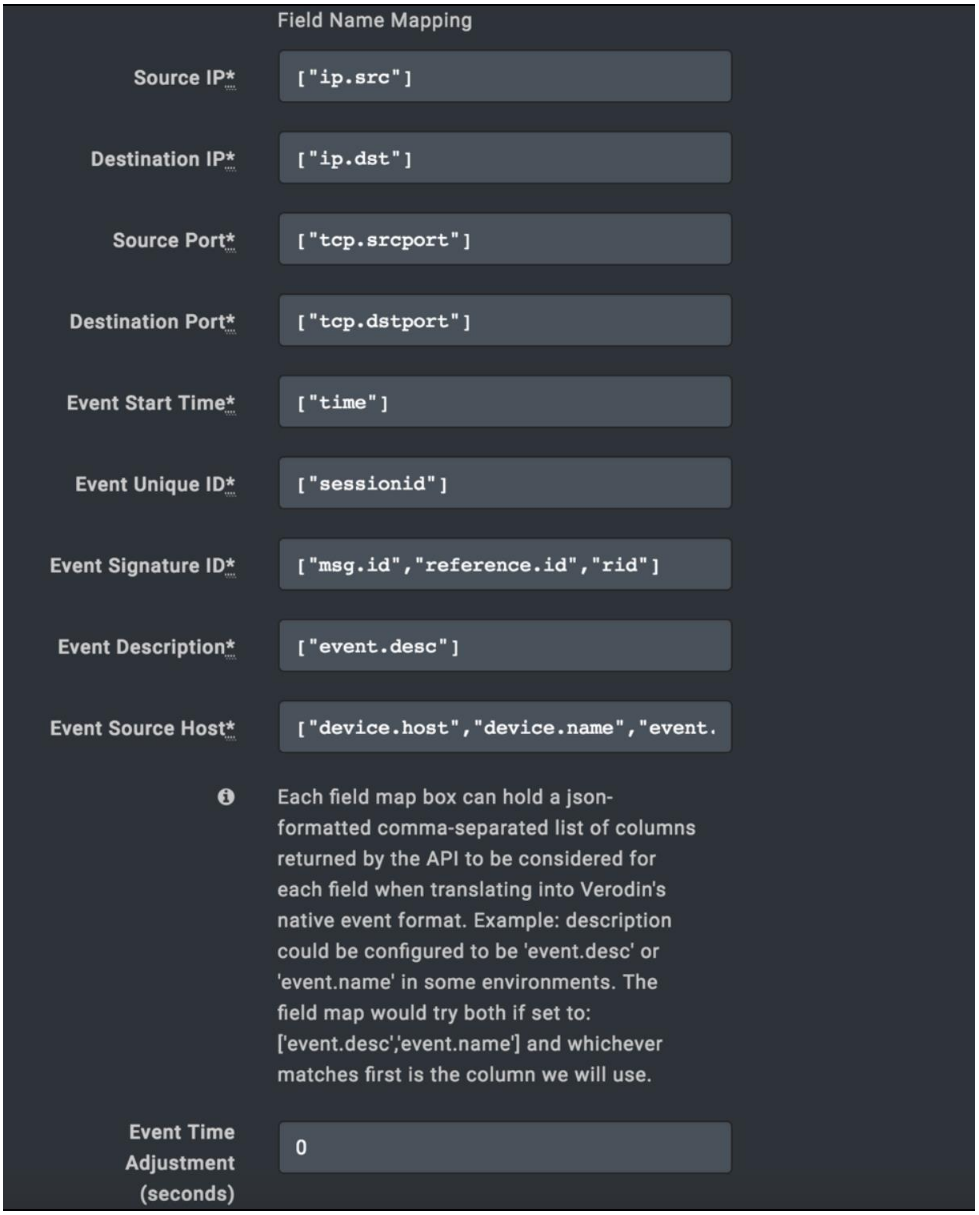
To add a new RSA NetWitness integration, click the **Add Integration** button and choose **RSA NetWitness**. Complete the applicable fields in the “Add RSA NetWitness” popup window, including the concentrator’s host **IP address, port, username,** and **password**. Click the **Submit** button:



Add RSA NetWitness

Host*	Host
Port*	50105
Protocol	http
Username*	Username
Password*	Password
Query	select * where time='%START_TIME%'-'%END_TIME%' && ((ip.src=%ACTOR_IPS%) || (ip.dst=%ACTOR_IPS%))

Advanced options are available for the RSA NetWitness integration, including field name mappings. Field name mappings are used to translate RSA NetWitness naming to Verodin's native field names. All inputs must be enclosed by square brackets [ ]. The inputs are used to list columns that can exist in an event. Enter a comma-separated list of the columns that could be used in an event in the appropriate text box. The first item in the list that matches will be used in Verodin. For example, in Event Description, the list: ['event.desc','event.name'] would try 'event.desc' first, and then 'event.name'.



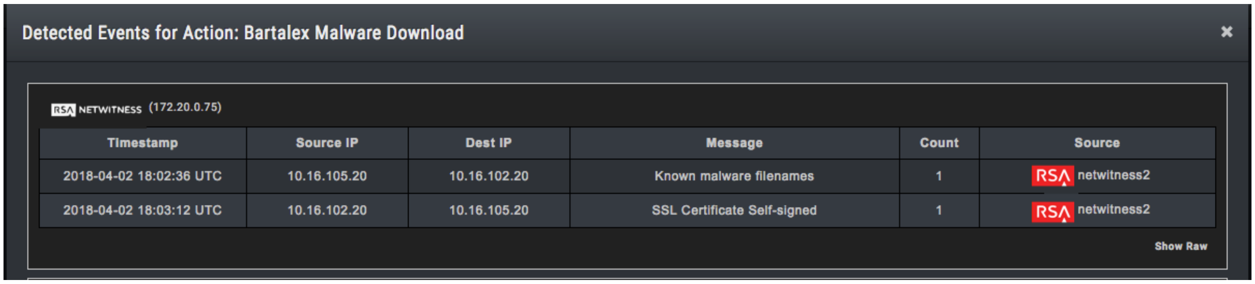
Field Name Mapping

Source IP*	["ip.src"]
Destination IP*	["ip.dst"]
Source Port*	["tcp.srcport"]
Destination Port*	["tcp.dstport"]
Event Start Time*	["time"]
Event Unique ID*	["sessionid"]
Event Signature ID*	["msg.id","reference.id","rid"]
Event Description*	["event.desc"]
Event Source Host*	["device.host","device.name","event.

ℹ Each field map box can hold a json-formatted comma-separated list of columns returned by the API to be considered for each field when translating into Verodin's native event format. Example: description could be configured to be 'event.desc' or 'event.name' in some environments. The field map would try both if set to: ['event.desc','event.name'] and whichever matches first is the column we will use.

Event Time Adjustment (seconds)	0

After receiving the events from integrations' queries, the Director parses the events and verifies they match the job's IP addresses, ports, and time. Those that match are viewable on the applicable Job page. However, if a raw event fails to match the Job's parameters, e.g. destination IP address data is missing, Verodin stores the data under the **Settings>Suspicious Events** page.



Detected Events for Action: Bartalex Malware Download

RSA NETWITNESS (172.20.0.75)

Timestamp	Source IP	Dest IP	Message	Count	Source
2018-04-02 18:02:36 UTC	10.16.105.20	10.16.102.20	Known malware filenames	1	RSA netwitness2
2018-04-02 18:03:12 UTC	10.16.102.20	10.16.105.20	SSL Certificate Self-signed	1	RSA netwitness2

Certification Checklist for RSA NetWitness

Date Tested: April 11th, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.5	Virtual Appliance
Verodin SIP		

RSA NetWitness Test Case	Result
Inline Query/Enrichment	
Query NetWitness for IP Info (source/destination IP)	✓
Query NetWitness for User Info (usernames, user behavior)	N/A
Query NetWitness for Specific Meta (Other)	✓
Retrieve NetWitness Log/Packet Data	N/A
Retrieve NetWitness PCAP files	N/A
Alerting / Incident Creation	
NetWitness alert via syslog	N/A
NetWitness alert via email	N/A
NetWitness alert via ESA/scripting	N/A
Send alert to NetWitness (Syslog, CEF, or custom parser)	N/A
RSA NetWitness Intel Feeds	
Update NetWitness Intel Feed (CSV, STIX)	N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function