RSA® NETWITNESS®
Implementation Guide

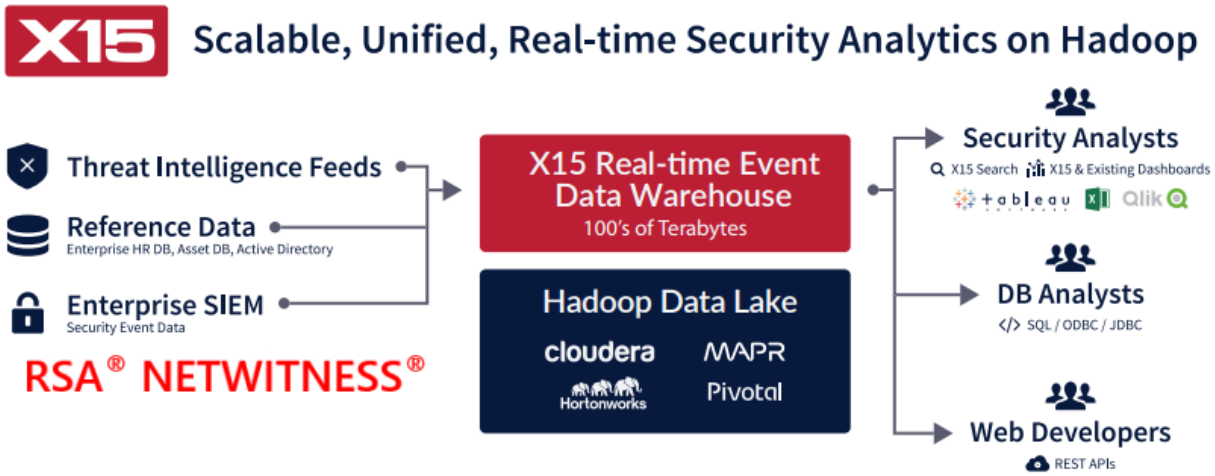
X15 Enterprise

Jeffrey Carlson, RSA Partner Engineering
Last Modified: January 23, 2017

RSA READY

Solution Summary

X15 Enterprise solves the complex problem of collecting and correlating large volumes of machine-generated data from network, security, and other infrastructure in real-time. Parallel computing, query optimization, integrated search and analytics, and real-time data availability are some of the key principles behind its patented architecture. By using X15 Enterprise to analyze RSA NetWitness data stored in the RSA Warehouse, the X15 platform provides a unified view across network operations to detect anomalies, investigate incidents, and audit compliance violations.



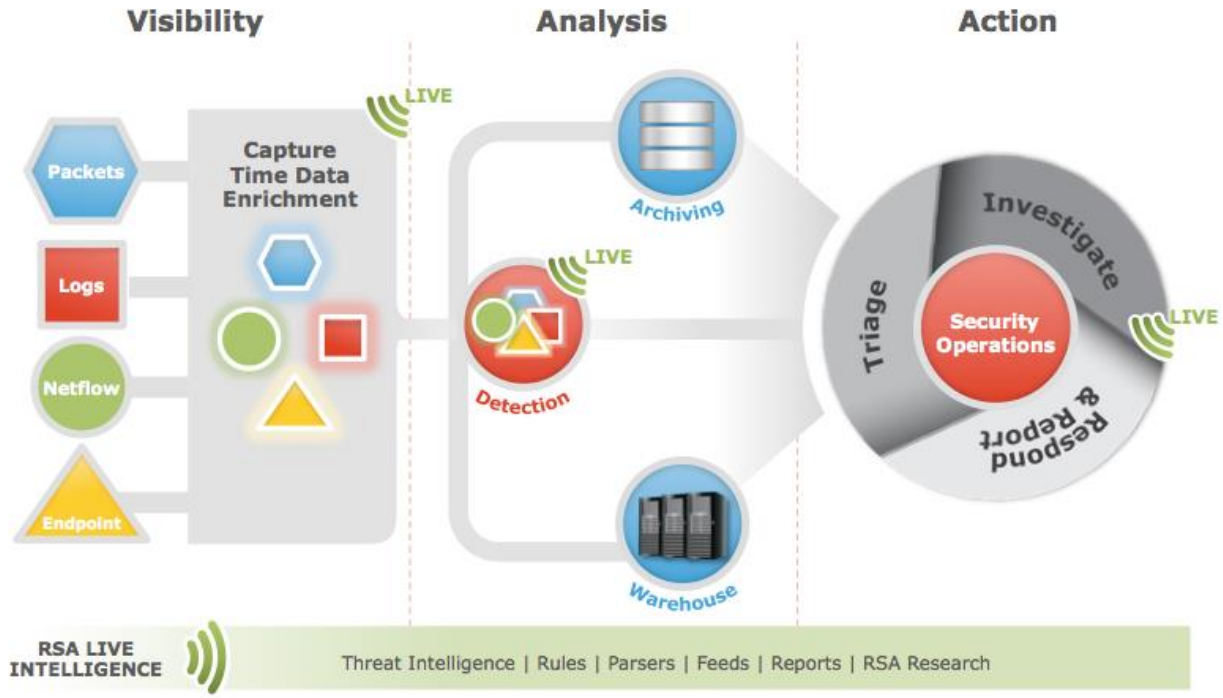
RSA NetWitness Configuration

RSA NetWitness Configuration

In order to integrate with X15 Enterprise, you must first have an RSA Analytics Warehouse installed and configured as part of your RSA NetWitness infrastructure. RSA Analytics Warehouse provides the capacity to process large amounts of current and longer term data through a Hadoop-based distributed computing system that collects, manages, and enables advanced analytics and reporting on Security Analytics data. RSA Analytics Warehouse requires a service called the Warehouse Connector to collect metadata and events from Decoder and Log Decoder and write them in Avro format into a Hadoop-based distributed computing system.

The Warehouse can be made up of three or more nodes depending on the organization's analytic, archiving, and resiliency requirements.

The following diagram depicts the architecture of a Security Analytics network that implements the RSA Analytics Warehouse component.



For more information on installing and configuring the Warehouse Connector, or for supported Hadoop environments, consult the **Warehouse Connector Overview** section of the RSA NetWitness product documentation at **https://sadocs.emc.com**

Partner Product Configuration

Before You Begin

This section provides instructions for configuring X15 Enterprise 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 X15 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 X15 Enterprise is properly configured and secured before deploying to a production environment. For more information, please refer to the X15 Enterprise documentation or website.**

X15 Enterprise Configuration

X15 offers a comprehensive system for storing and analyzing all enterprise data types within a single modern big data repository built on HDFS and abstracting away the complexity so that security operators do not also need to become Big Data experts to use it. The simpler X15 integration model saves substantial time, resources and money, especially when compared to the effort involved in integrating disparate open source computing frameworks within Hadoop.

Getting Data In

X15 provides various lightweight data ingestion agents for importing raw data along with other extracted fields. Data can reside anywhere in the network on any filesystem.

For example, data residing in HDFS can be loaded onto X15 by using the *hdfsloader* utility. The *hdfsloader* is a command line utility which can be executed from anywhere as long as it has access to the HDFS system as well as the X15 cluster.
This permits accessing Warehouse data in HDFS of any format including *AVRO*.
Given the path pattern to include or exclude a file, the hdfsloader ingests the contents of the files into X15. *Note: File change notifications are not available with HDFS mode.*

Run ./hdfsloader to see a complete list of options. Here is a typical *hdfsloader* command:

sh /opt/x15/tools/bin/hdfsloader 'database_name' 'table_name' "hdfs://localhost:9000" -ingestor-host-pool localhost -path-list /typical-warehouse-path -finished-files-path /file_status

Options database, table, "hdfs-uri", "-ingestor-host-pool", "-path-list" are required.

Similar to *hdfsloader* the *filemonitor* utility is used to monitor and ingest data from regular files or entire directories outside of HDFS. As in the *hdfsloader* case the *filemonitor* can be executed from anywhere the

data resides as long as it can communicate with the X15 cluster. Here is an example of a *filemonitor* command:

sh /opt/x15/tools/bin/filemonitor 'db_name' 'table_name' --path '/data_path' -mp '/path_to_file_history'

X15 Enterprise

Once the connector has been configured, analysts can use X15 Enterprise to search huge sets of raw data in order to quickly find the needle in the haystack and then perform further SQL-based quantitative analysis on the resulting records to gain deeper insights into a threat.

In *Figure 1.1* below you can see a set of sample data loaded into a table named **rsa_data**:

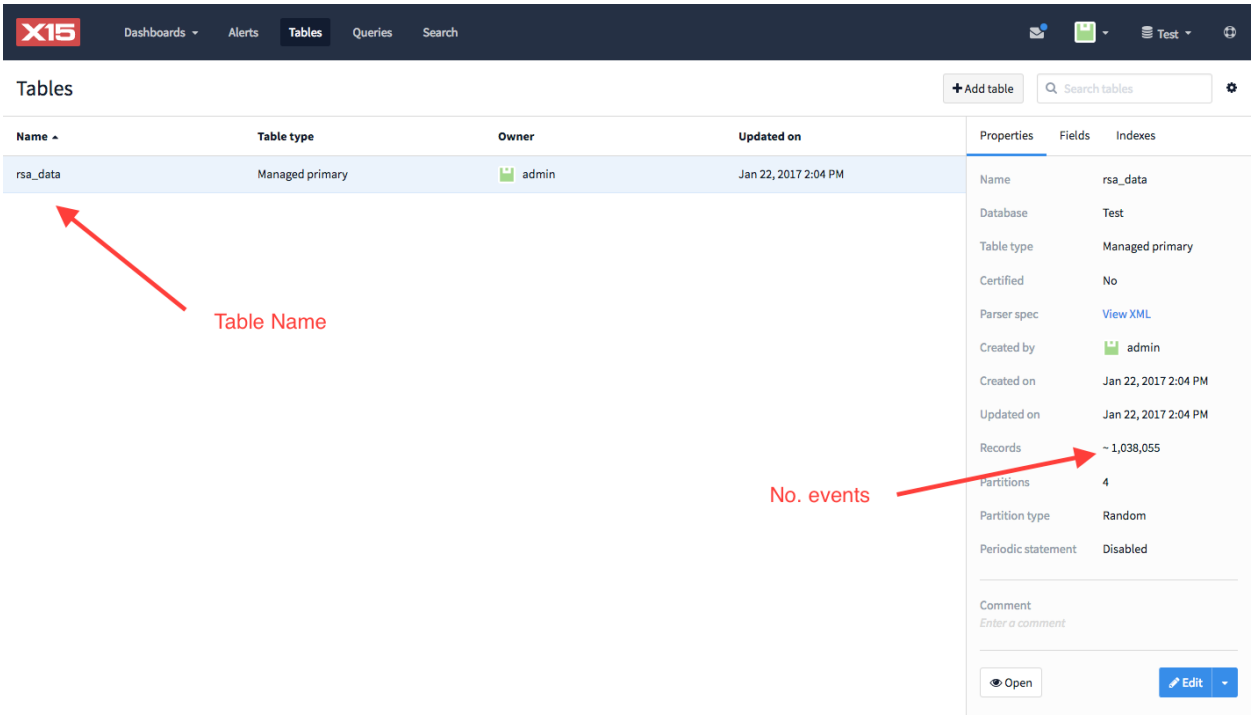


Figure 1.1 - New table with RSA data

Click the *'Open'* button, bottom-right, to view the contents of this table in the *Search* view. Notice the search bar is automatically populated with a *'SELECT * FROM'* statement. Below that, a timeline chart shows the number of events over time. On the left drawer there is a list of all the available fields extracted. At this point we are ready to start analysing our data as well as create and save charts right from this view. *See Figure 1.2 below.*

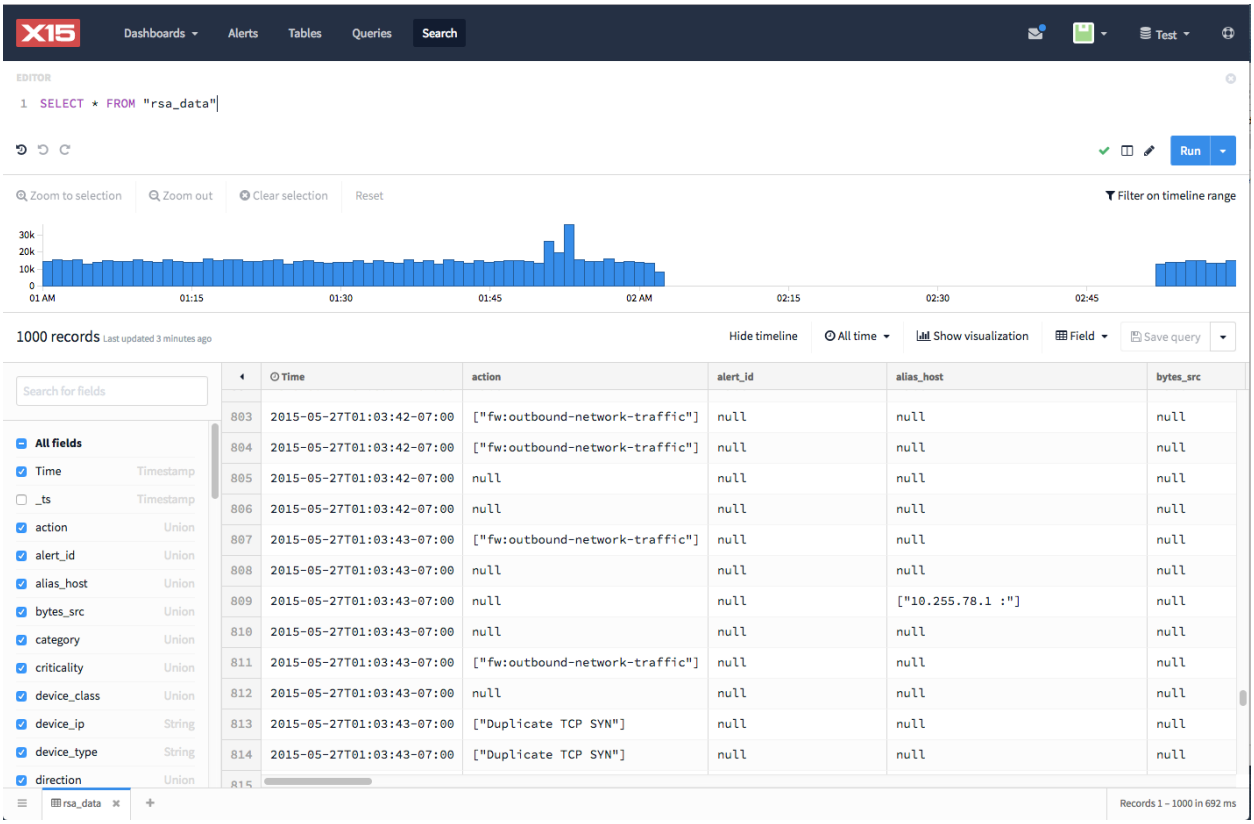


Figure 1.2 - A view of all fields in our table.

A quick way of looking at the rsa data distribution by device class would be to issue the following query: (SELECT * FROM "rsa_data") | top device_class
This is a combination of SQL syntax with X15's pipe-delimited language (XPL). This quickly returns a count of events by device_class and their corresponding percentage. *See Figure 1.3 below.*

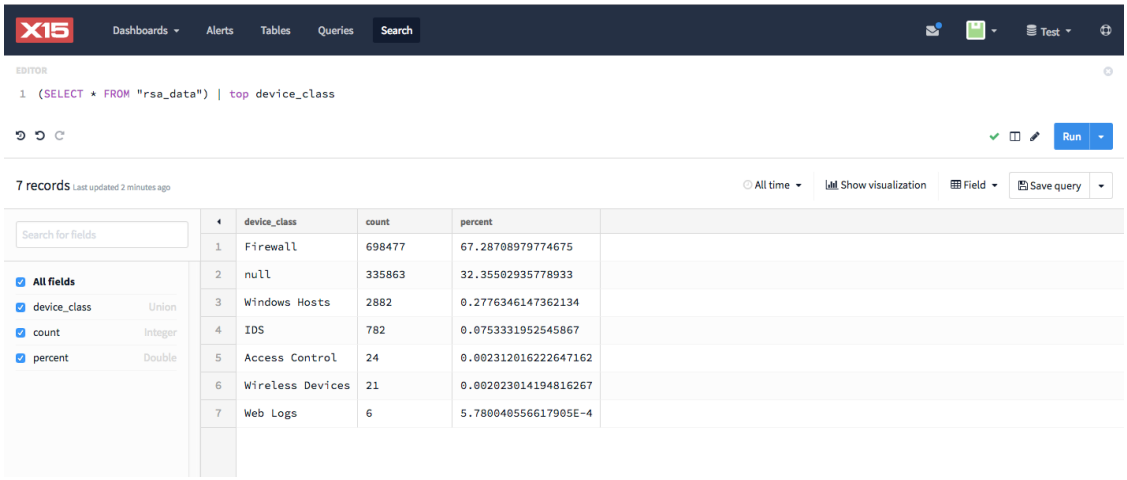


Figure 1.3 - top device_class

We have added another table of known blacklisted ip's into X15. *Figure 1.4* shows our newly added table 'blacklist_ips' containing ~7k records.

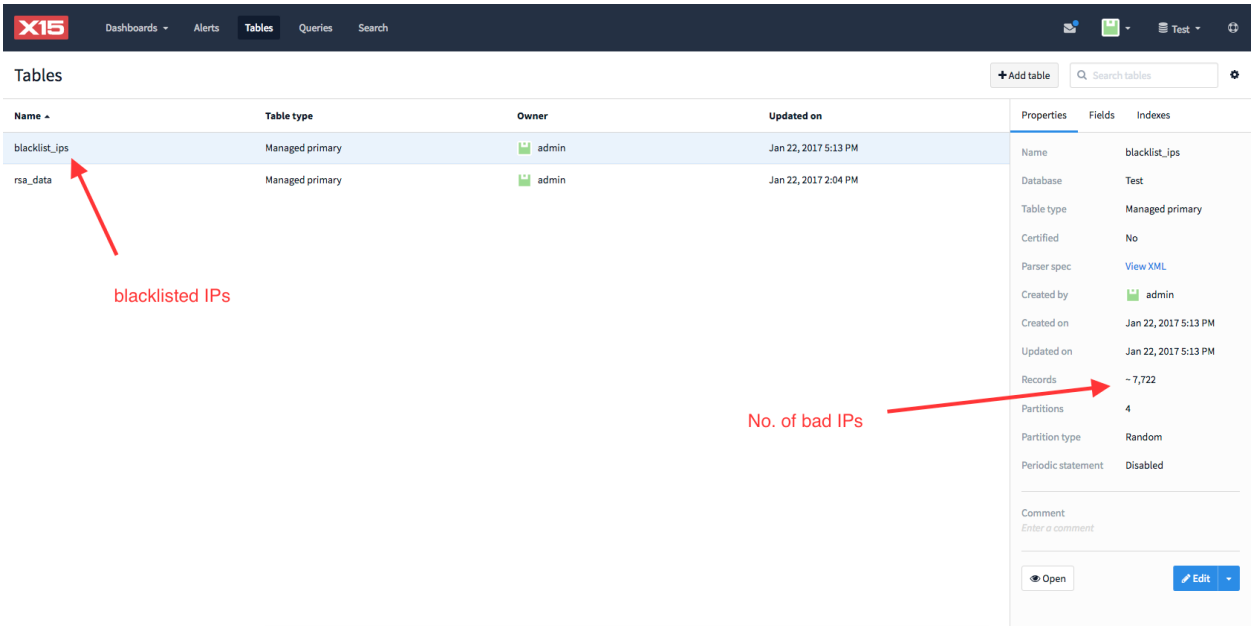


Figure 1.4 - blacklist_ips table added

A common exercise is usually filtering out records which contain a blacklisted ip. In our case we will use the 'blacklist_ips' table as a reference table and join it with 'rsa_data'. For example let's join the 'rsa_data' table and 'blacklist_ips' on the predicate 'ip_dst'='bl_ip' as in *Figure 1.5:*
SELECT * from "rsa_data" a join "blacklist_ips" b on a.ip_dst = b.bl_ip

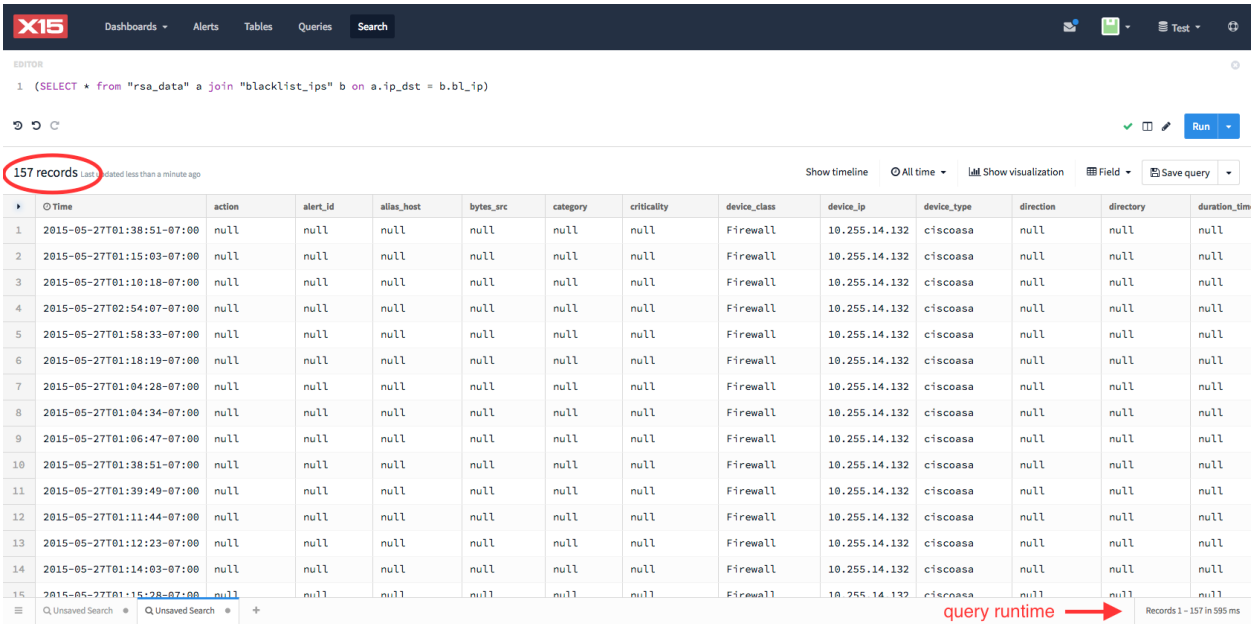


Figure 1.5 - Check ip_dst if it contains blacklisted IPs.

The above search looked for matches of the ip_dest field against the blacklisted IPs. What if we need to find out if any of the blacklisted IPs are to be found anywhere in the raw_log field of the 'rsa_data' table? For that we utilize the @@ operator which allows X15 to search the index for values coming from the blacklisted IPs table. In addition we will combine this new join query with the XPL 'top' command on the countryID. Run the following search:
(SELECT * FROM "rsa_data" a join "blacklist_ips" b on a.raw_log @@ 'b.bl_ip') | top countryid
See Figure 1.6

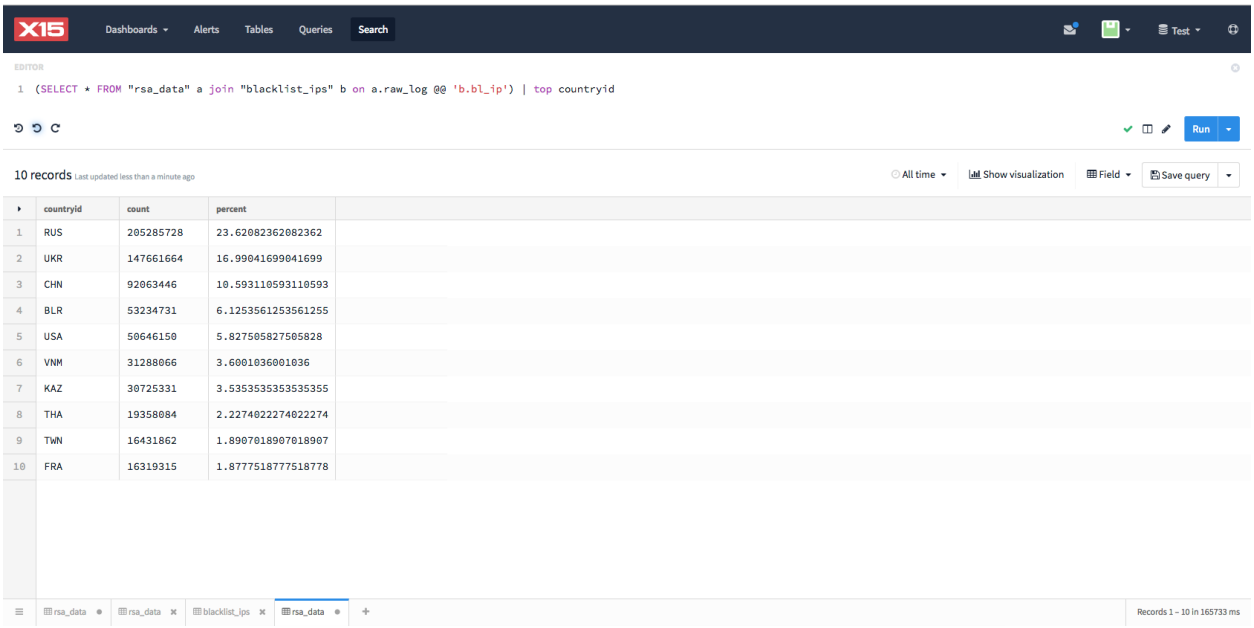


Figure 1.6 - Top blacklisted sources by Country

On the same *Search* view we will now create a chart based on the last results. Click on Show visualization. A list of options for X & Y axis and data Series is presented on the left hand side. *See Figure 1.7.* The table results can still be seen on the bottom of the screen. Once the chart representation is complete we can save the chart as a widget in a new or existing dashboard via the menu on the right as shown below in *Figure 1.7.*

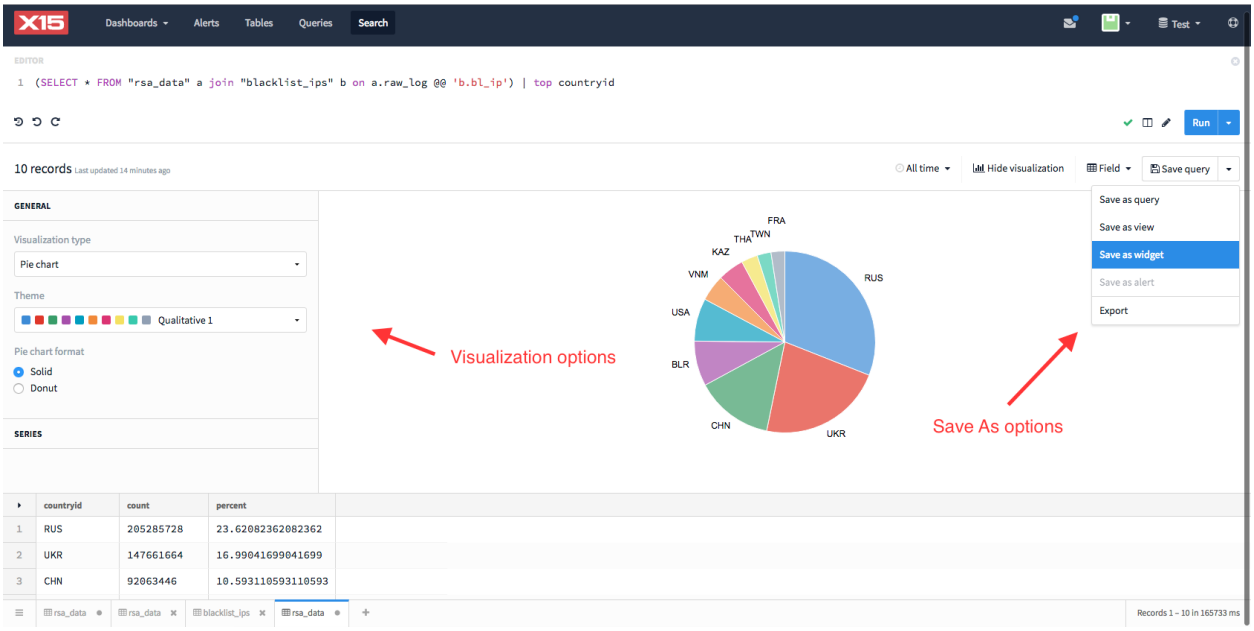


Figure 1.7 - From 'search'-to-'chart' workflow

Conclusion

X15's Real-time event data warehouse for Hadoop offers a robust complement to existing security solutions. Organizations can leverage the RSA NetWitness Suite for tried-and-true correlation and operational security monitoring capabilities, while using X15 for security analytics at massive scale – flexibly spanning diverse data, for historic and real-time ad-hoc forensic analysis.