Vorstack
Vorstack ACP

RSA Security Analytics Ready Implementation Guide

Last Modified: January 28, 2015

Partner Information

Product Information	
Partner Name	Vorstack Corporation
Web Site	www.vorstack.com
Product Name	Vorstack ACP
Version & Platform	v5.1
Product Description	Vorstack Automation and Collaboration Platform (ACP) is a distributed analytics and global correlation platform for multi-party coordinated cyber defense. Vorstack ACP increases operational efficiency by automating the process of analyzing incoming threat data thereby reducing discovery time, remediation time, and overall risk. Combined with Vorstack's secure and anonymous collaboration, we give you the control and auditability needed to satisfy strict domestic and international requirements to allow for true security-threat information sharing.

Solution Summary

Overview

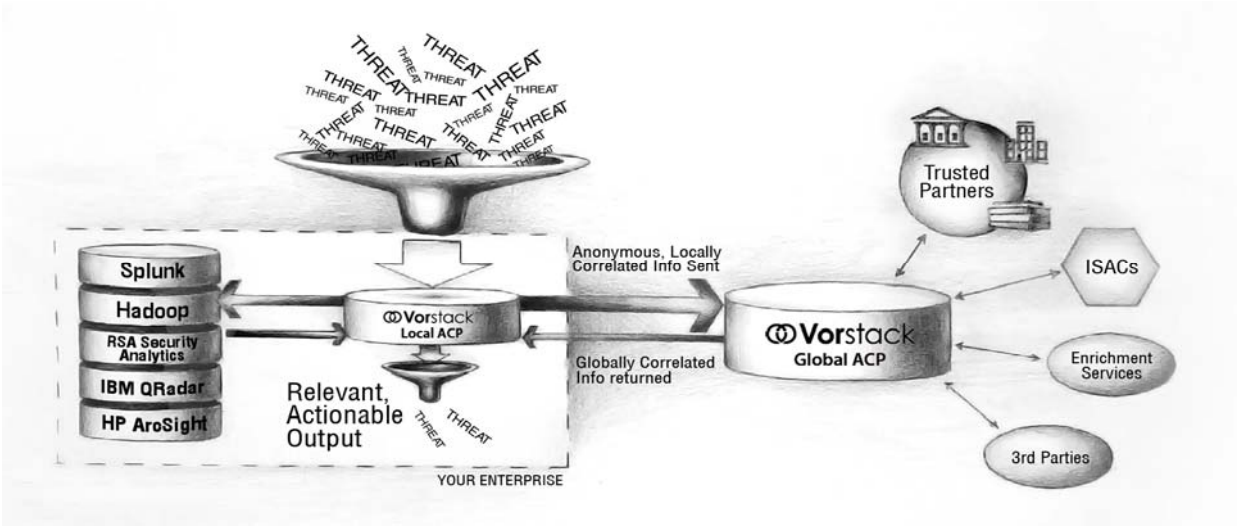
The Vorstack ACP enables you to automate the consumption of threat indicators, correlate them against data that is stored in your RSA Security Analytics, add 3rd party enrichment, such as reputation, to the data and understand the prevalence and history of those indicators amongst your trusted peers and the Vorstack community. Threat indicators can be consumed from unstructured (e.g. emails) as well as structured data sources (e.g. threat feeds, threat repositories). The results of the correlation and enrichment can be presented in email, on the ACP dashboard or integrated into your workflow with our set of RESTful APIs.

Deployment

The Vorstack ACP is deployed as a virtual machine in a VMWare VSphere environment much like RSA Security Analytics. The ACP uses the Security Analytics SDK to make queries through the main Broker in the deployment. The customer just needs to configure the URL that points to the Broker, the user credentials, and, if necessary, adjust the search configurations for threat indicators of interest (IPs, URLs, hashes, etc). Once the RSA Security Analytics configuration is complete, the user configures the sources of threat information they want to use (email, integrated open source threat feeds, STIX repositories, etc) and they are able to start automatically correlating with their data. Additionally they can join "Trusted Circles" to share threat information with trusted peers.

Business Case

There is currently an explosion of threat information available today. The problem for security analyst and the CISO that he or she reports up to is to understand what of that threat information is relevant and useful to them. While SIEMs like RSA Security Analytics do a great job looking at the data in the customer's environment for known bad patterns, etc. they can be augmented with a system that allows the ingestion of new, timely sources of information, whether they are structured repositories, like STIX objects delivered over a TAXII feed; emails, like FBI flash reports in PDF; or threat information generated directly by a trusted peer. Having the ability to quickly correlate this threat information, which has been enriched with additional information about those threat indicators, with data in the customers environment allows the customer to go from "indicator to incident" much faster than before freeing up the security analyst to spend time on the detailed forensic investigation using the tools available in RSA Security Analytics.



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Vorstack ACP with RSA Security Analytics. 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 Vorstack ACP components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

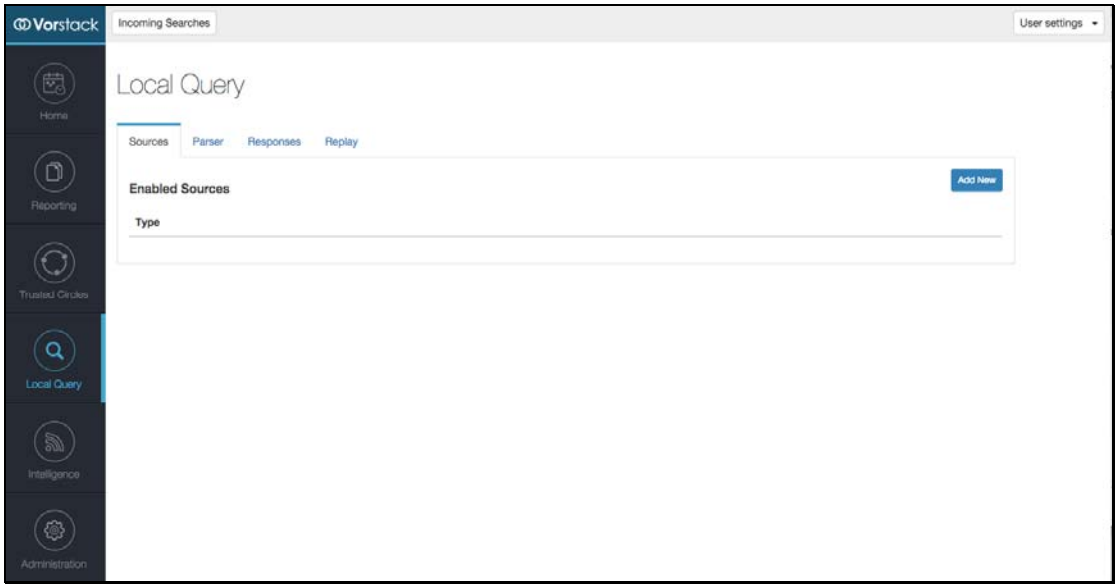
Vorstack ACP Configuration

Connecting to the SIEM or Log Store

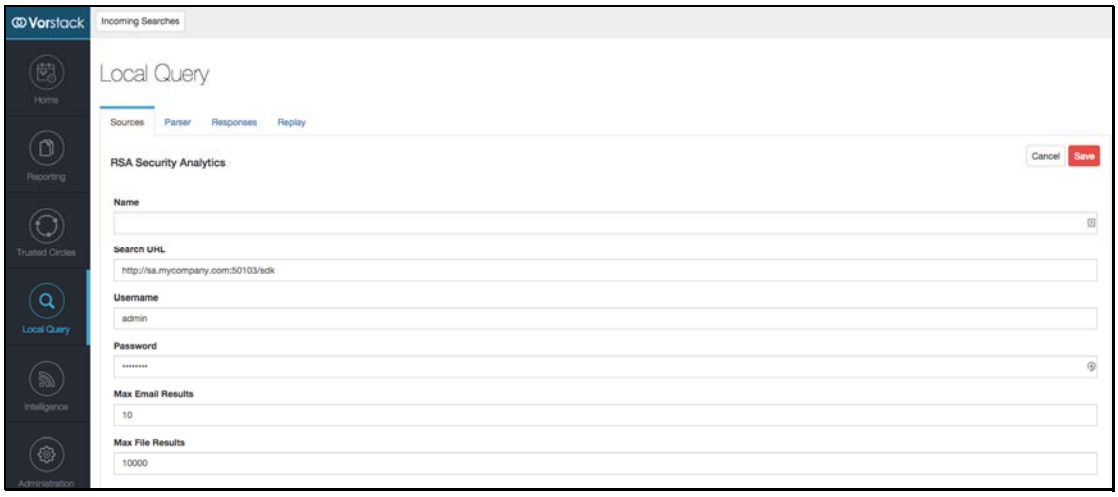
Connecting to the SIEM or log store requires that you provide authentication credentials for API access to the system as well configure queries for each indicator type that you are interested in searching. The Vorstack ACP comes preconfigured with a number of standard indicators listed in the table below (see Advanced Configuration to learn about adding your own custom indicators). For many of these, there are default queries available when you configure your SIEM or log store. You should review the queries to make sure they are appropriate for your environment.

Attribute Name	Description
md5,sha1	hash
ip_addr	IPV4 address
url	URL
domain	Domain
credit_card	Credit Card Number
phone	Phone Number

1. To configure, select the **Local Query** menu, and on the first tab select **Sources**.
2. Select **Add New** to configure the source.
3. Select **RSA Security Analytics** from the list of sources.



4. Using the following screen captures configure the following;
   - Authentication and Connection
   - Search Definition
   - Connection Testing



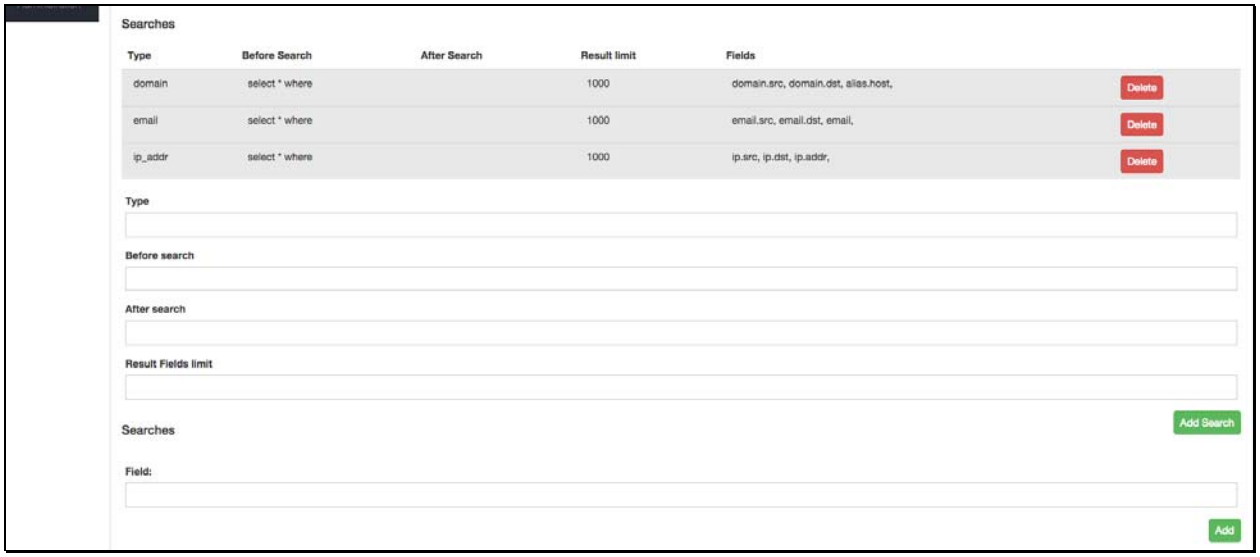
5. Most items in the authentication and connection section of the page are self-explanatory.

> **Note: The "Max Email Results" determines how many rows of RSA Security Analytics data are passed to the email template for data that gets emailed back to the user. This data will only be seen in situations where the email template renders detailed data. If you have any questions about email templates, please contact your Vorstack representative.**
>
> **The "Max File Results" determine how many rows of data are saved as a file that can be downloaded from a link in email, the user interface or through the API.**

6. To add a search for a new Type of indicator, specify the indicator **Type** (as described in the Parser).
7. Specify the list of fields and indicator values within the **Before Search** field.
8. Specify the list of fields and indicator values within the **After Search** field and set a numerical limit to the number of results that should be returned from the query.
9. Finally, enter the search Fields, as defined by Security Analytics, one at a time with the **Add** button.

> **Note: The "Searches" section allows you to specify what search is performed when an indicator of type "Type" is sent into the system.**

10. After completing the Searches form, click the **Add** search button to register the search for a new search type.



11. To test the connection to the RSA Security Analytics server, enter the **Search Type** and **Value** before selecting **Test Connection.**
12. Click **Save**, to store the connection.