RSA® NETWITNESS®
SafeBreach
Integration Guide

SafeBreach

Bharath T R, RSA Partner Engineering
Last Modified: May 20, 2020

RSA READY

Solution Summary

SafeBreach simulates attacks to see whether they are blocked in the network. When you use the SafeBreach automated analysis, relevant logs are correlated with simulation results to create a consolidated status of each simulation.
Users can drill down to see which security controls were involved in blocking or detecting the breach as well as the rules and events that led to the result.

SafeBreach Configuration

Before You Begin

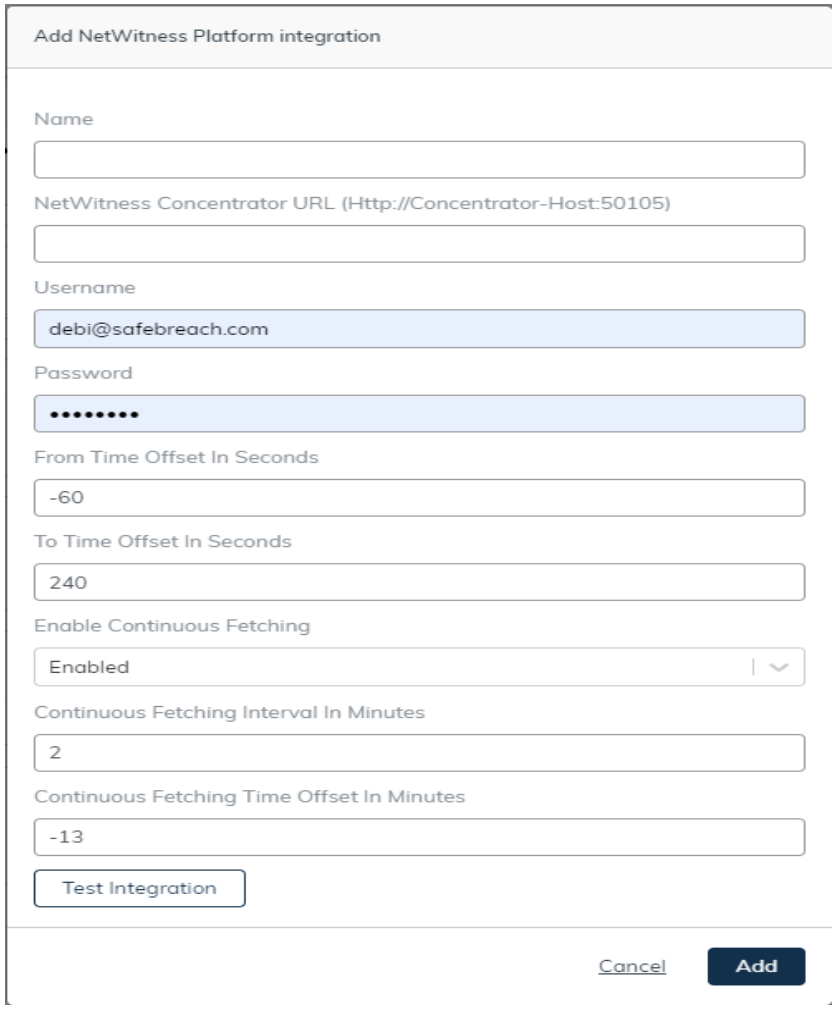
- Check that SafeBreach Management has connectivity with RSA NetWitness.
- Run appropriate simulations to make sure that logs are generated in the security control you wish to integrate. Otherwise, troubleshoot detection or contact SafeBreach support.
- *Obtain user credentials with API permissions* for API calls.

Add the RSA NetWitness Integration on SafeBreach Management

Integrate RSA NetWitness with SafeBreach Management:

1. Click **Administration** and select **Integrations** from the left pane menu.
2. Select **RSA NetWitness Platform** from the **Add Integration** drop down menu.

   The **Add NetWitness Platform integration** window is displayed.



3. Fill in the required fields, as described in the following table.

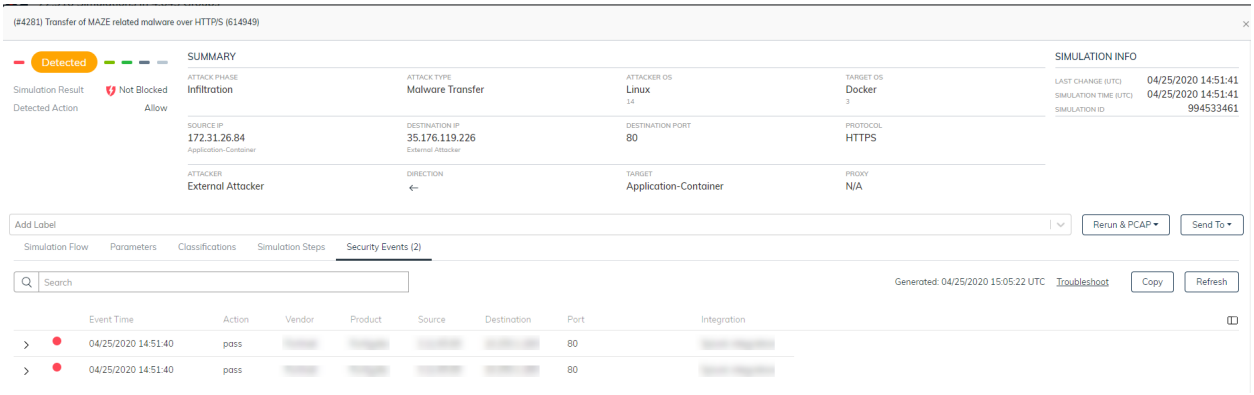
Parameter	Details
Name	A name for the RSA NetWitness integration
NetWitness Concentrator URL (Http://Concentrator-Host:50105)	The URL to which SafeBreach sends API calls
Username	The name of the customer's RSA NetWitness console
Password	The secret to be used for authorizing access to the RSA NetWitness integration
From Time Offset in Seconds	The number of seconds relative to when the simulation was completed to begin the security control query. The default is **-60**, that is, 60 seconds before the simulation was completed. The minus indicates back in time from the simulation
To Time Offset in Seconds	The number of seconds relative to when the simulation was completed to end the security control query. The default is 240 (4 minutes).
Enable Continuous Fetching	Enable this parameter to retrieve security events for simulations as they occur. In this way, the status of simulations provides an integrated, correlated view of the simulation results and detected security events and an aggregation of results are displayed in the Test Summary. When **Continuous Fetching** is disabled, the security events are only be retrieved when you drill down on a simulation in **Simulation Results**.

4. Test the configuration by clicking on **Test Integration** and correct the settings, if required.
5. Click **Save**.

Validation

In order to validate the simulation details:

1. Run a plan or other test with attack types that are relevant to the security controls being validated.
2. View the simulation details, including the **Security Events** tab with the correlated events.



3. Identify the relevant log in RSA NetWitness and compare the parameters to ensure that they are the same as the log displayed in the **Security Events** tab of the relevant simulation result. If there is a discrepancy, contact SafeBreach Support.