ANOMALI – RESILIENT INTEGRATION GUIDE

V1.0

Copyright Notice

Table of Contents

1. Introduction

Threat Intelligence provides valuable incident context to help incident responders to reduce investigation time and enable a rapid, decisive response. Anomali ThreatStream offers the most comprehensive Threat Intelligence Platform, allowing all threat intelligence feeds to be managed and automatically made available to your security team in real-time. By integrating ThreatStream and the Resilient Incident Response Platform, your security team is able to gain instant context regarding artifacts associated with an incident.

This guide describes how to integrate Anomali ThreatStream with the Resilient Incident Response Platform.

2. Overview

As part of Resilient's incident response, artifacts (or evidence) may be added to an incident for tracking and analysis. Using the Resilient Custom Threat Service, Anomali ThreatStream integrates with the Resilient platform so that any network artifacts you add to any Resilient incident automatically performs a ThreatStream enrichment lookup to provide additional information regarding the artifacts.

Figure 1 is an example of ThreatStream lookup results shown in Resilient (1).

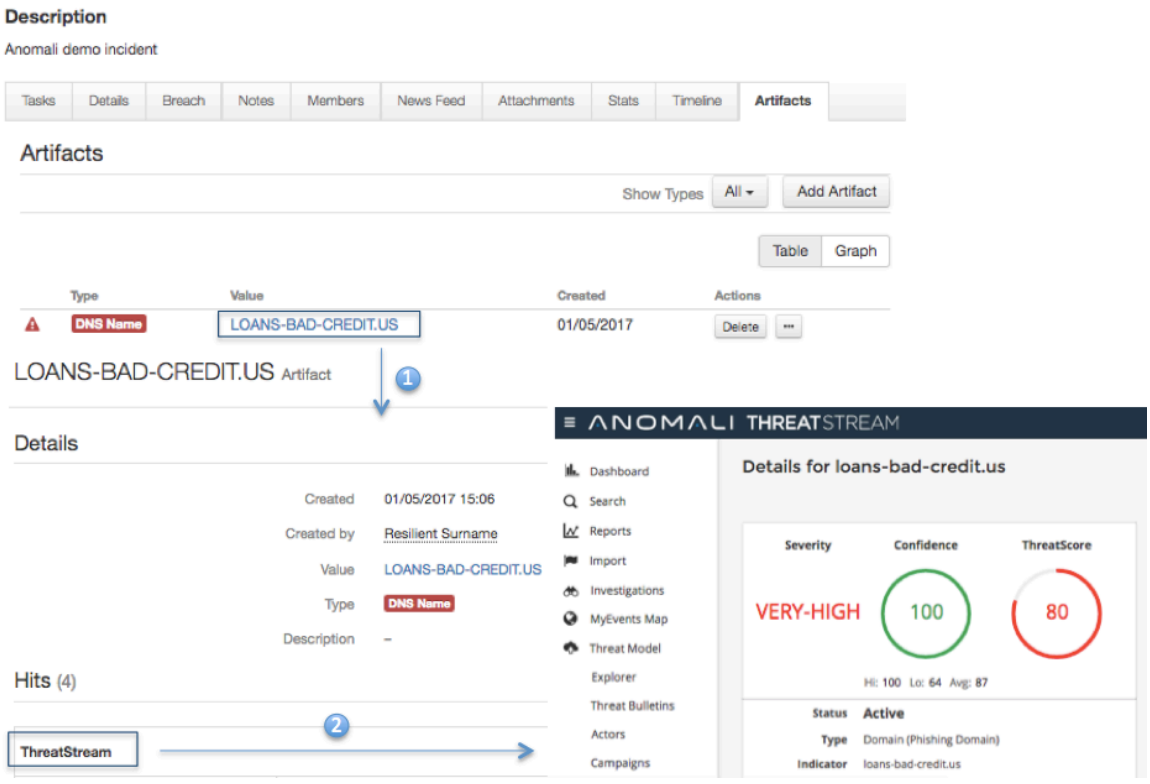


Figure 1 Example of ThreatStream/Resilient IRP Integration

In this case, the security team adds loans-bad-credit.us as an artifact to an incident in Resilient for investigation and analysis. The integration automatically performs a look-up into ThreatStream and returns search results with details about the artifact (e.g. status, threat type and score, and intelligence resources). ThreatStream provides the essential analysis and correlation to translate raw, unstructured and duplicative data into true intelligence, and reduce the noise of false positives from outdated irrelevant data. The integration is built to return results for artifacts that are active and actionable. Figure 1 shows that loans-bad-credit.us is an active Phishing domain with high scores of maliciousness reported by multiple credible sources including Anomali Labs and several commercial intelligence providers (under the condition of active feed subscriptions).

To conduct further threat analysis, the security team can launch into the ThreatStream portal (2) to gain additional context (actors, campaigns, TTPs) and leverage the threat models (kill chain, diamond model and STIX/TAXII) to assess the nature and scope of the threat to make informed decisions.

3. Prerequisites

Before registering Anomali ThreatStream as a threat service with the Resilient platform, verify the following:

- The Resilient platform is version v26 or later.
- The Resilient platform is connected to the internet.
- You have a master administrator account with the Resilient platform.
- You have access to the command line of the Resilient appliance, which hosts the Resilient platform.
- You have an Enterprise account from Anomali ThreatStream. To obtain an Enterprise account, contact your Anomali representative or register with Anomali ThreatStream at https://ui.threatstream.com/login. Once logged into the ThreatStream portal, navigate to Settings -> Profile Settings to locate your ThreatStream API key.

4. Register the Threat Service

Perform the following to register the Anomali ThreatStream as a Resilient custom threat service:

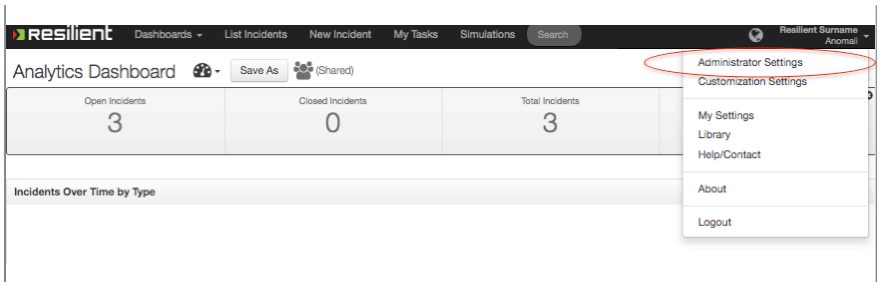
1. Log in to the Resilient appliance using an SSH client, such as PuTTY.
2. At the prompt, enter the following command.

```
sudo resutil threatserviceedit -name ThreatStream -resturl
'https://api.threatstream.com/api/v2/intelligence/resilient_search/?username=
USERNAME&api_key=API_KEY'
```

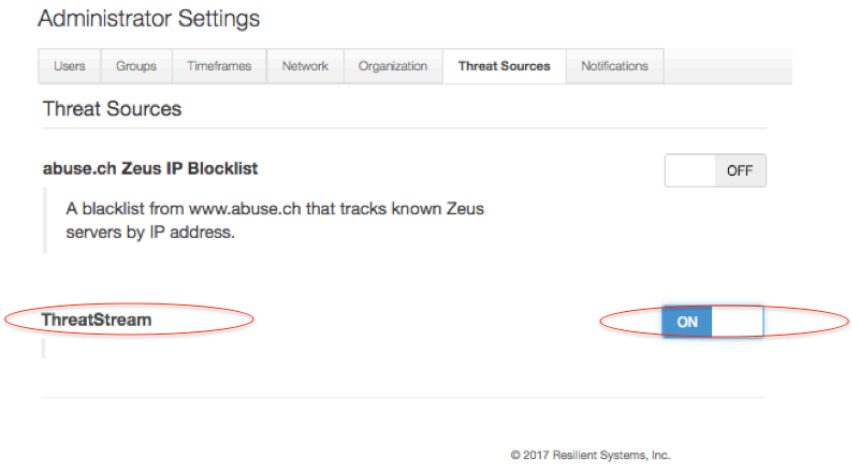
3. Once completed, test the connectivity using the following command. If the previous step was successful, you should see a success message.

```
sudo resutil threatservicetest -name "ThreatStream"
```

4. Log into the Resilient platform as a master administrator then click on your username and select **Administrator Settings** in the drop-down menu.



5. Click the **Threat Sources** tab and scroll down until you find ThreatStream. Make sure that it is set to **ON**.



NOTE: If you need to disable the Anomali ThreatStream threat service, you can turn the threat service to OFF.

If you need to remove the threat service, log in to the Resilient appliance using an SSH client and type the following command:

```
sudo resutil threatservicedel -name "ThreatStream"
```

5. Customer Support and Feedback

Please contact support@anomali.com for any questions or feedback.

6. About Anomali

Anomali delivers earlier detection and identification of adversaries in your organization's network by making it possible to correlate tens of millions of threat indicators against your real time network activity logs and up to a year or more of forensic log data. Anomali's approach enables detection at every point along the kill chain, making it possible to mitigate threats before material damage to your organization has occurred. Headquartered in Redwood City, Calif., the company is privately held and has received venture capital backing from General Catalyst Partners, GV, Institutional Venture Partners, and Paladin Capital Group, as well as individual investors. To learn more, visit www.anomali.com and follow us on Twitter: @anomali.

7. About IBM Resilient

Resilient's mission is to help organizations thrive in the face of any cyberattack or business crisis. The industry's leading Incident Response Platform (IRP) empowers security teams to analyze, respond to and mitigate incidents faster, smarter and more efficiently. Part of IBM Security, the Resilient IRP also integrates security technologies into a single hub and provides an orchestrated workflow spanning an organizations people, process and technology driving down response time. With Resilient, security teams can have best-in-class response capabilities. Resilient has more than 130 global customers, including 30 of the Fortune 500 and partners in more than 20 countries. Learn more www.resilientsystems.com.