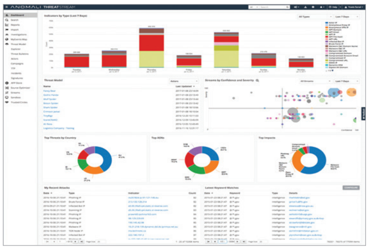
SC MEDIA ★★★★★



Anomali

ThreatStream

DETAILS

Vendor Anomali

Price Starts at $5,000

Contact anomali.com

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★¾
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Solid collection of feeds and indicators of compromise.

Weaknesses We would like to see a broader collection of supported third-party security devices.

Verdict Solid threat intelligence product with a prodigious collection of resources. Fits well into just about threat and intelligence analysis tool set. At a price that is hard to beat, we make this our Best Buy.

Anomali ThreatStream is a threat analysis SaaS platform that also has an on-premises option supplied as a virtual machine for those organizations that don’t want to risk a cloud-based deployment. The tool includes over 140 open-source feeds and allows easy inclusion of commercial feeds through the Anomali APP Store. We found the feeds to be typical of the open-source feeds with which we are familiar, but it is unusual to have such a wide variety of choices. Taken with the available commercial feeds – which must be paid for, of course – the underlying threat sources are a significant plus.

SC MEDIA BEST BUY

ThreatStream includes a built-in sandbox allowing files to be submitted and analyzed. You also can import such files as intelligence reports or lists of IoCs. The product can be integrated with many popular SIEMs and includes a case management feature for assigning research tasks, supporting an analyst workflow, and allowing collaboration with trusted partners. ThreatStream Link allows you to share intelligence directly with devices on your enterprise. This allows links to SIEMs and supports both Windows and Linux platforms.

We dropped into the landing page and found a typical status dashboard. Everything that you need for the big picture is there, and you can drill down for lots more data. Drilling down exposes indicators, such as IP, hash values and domains. Currently there are about 216 different indicators. This is the meat and potatoes of any intelligence system – the completeness of its indicator library. Taken with the large number of available feeds this makes a powerful tool, indeed.

Drilling down into the indicators, we saw significant detail. We saw a detailed description about an actor named Dynamite Panda (among other names). The tool is fully Stix-compatible using their REST API for imports and exports. We fed it a name of an actor who we knew to be fairly new on the underground scene and it had information about him. The forum where we found this particular actor showed him as being active from January 17 and at the time we looked it was only Jan. 23.

Investigation reports can be output in STIX, Kill Chain or Diamond format to meet your analysis style. We found the price reasonable, especially in light of the obvious benefits this tool offers. We wish that it was able to integrate with a wider variety of tools. It does integrate with Splunk, however, so that can provide some useful additional tools where the platform does not have a direct integration. Support is as one would expect. However, you need to be an existing customer to access the support portal. To make up for that there is a resources page on the website that will get you a lot of what you need. The company provides basic no-fee support from 3 a.m. to 10 p.m.

ANOMALI™

Anomali
808 Winslow Street
Redwood City, CA 94063
844-4-THREATS • www.anomali.com

Reprinted from **SC Magazine, March 2017** • www.scmagazine.com