One-stop shopping for threat intelligence, courtesy of ThreatStream

Analyst: Wendy Nather
13 Oct, 2014

For a loose definition of ‘threat intelligence,’ you might consider antivirus signatures to have been the first generation of commercial data about attacks. The industry has moved on by light years since then, but it still has to differentiate itself from those humble beginnings. Threat intelligence vendors today have to win several races: to have the most varied types of data, to have the largest collaboration membership, and to be the ‘one ring to rule them all.’ ThreatStream is tackling those challenges with several offerings that go beyond the data itself.

The 451 Take

ThreatStream has a significant ArcSight pedigree, including Hugh Njemanze, who has now taken the reins as CEO. There are many threat intelligence rivals that want to be the hub, but the company has taken steps to differentiate itself in the form of offerings such as an easy-to-deploy 'honeynet' for customers, followed by the recent announcement of its Alliance Preferred Partner (APP) store for other commercial feeds. ThreatStream recognizes that just connecting to SIEMs isn't enough, and that a collaboration platform depends on a potentially fickle set of users. It has to keep innovating to maintain its visibility in the market.

Context

ThreatStream was founded in early 2013 by Greg Martin with seed money from Njemanze (founder and former CTO of ArcSight) and Tom Reilly (former CEO of ArcSight and now CEO of Cloudera). The company moved its headquarters from New York City to Redwood City, California, and in February announced a series A round of $4m led by Google Ventures, with participation from Paladin Capital, Njemanze and Reilly. Martin moved over to the CTO role in July so that Njemanze could take the
helm; the company is up to 30 employees.

**Products and services**

ThreatStream has rebranded its threat intelligence analysis and sharing platform as Optic; it ingests threat intelligence (currently more than 100 free open source and commercial feeds) and uses its own algorithms to automate the classification of malware and threat actors, among other information. In order to grow the community, the company makes a free version of Optic available that includes the feeds and sharing. The premium Optic service includes OpticLink, the integration with SIEMs and other security infrastructure (currently supporting ArcSight, Splunk, NitroSecurity/McAfee and Q1 Labs/IBM). Licensed as an annual subscription, and priced based on the number and size of SIEM instances the customer is using, Optic runs anywhere from $60,000-260,000 per instance. The company says it has 25 paying customers, as well as 700 customer entities using the free Optic version.

In June, ThreatStream announced its Modern Honey Network, an open source management platform that enables enterprises to deploy their own honeynets more easily. Not only can the customer track who's trying to attack it through those collections of decoy systems, but it can also send the data to ThreatStream to include in its own intelligence. The vendor says it has had more than 10,000 downloads and deployments of the Modern Honey Network.

Most recently, ThreatStream announced a new APP store for threat intelligence; the marketplace features commercial intelligence feeds from vendors such as CrowdStrike, Emerging Threats, Farsight Security, Flashpoint Partners, ReversingLabs, Team Cymru and Webroot. Customers can purchase the feeds and have them integrated with Optic. ThreatStream emphasizes that it can offer better-quality threat intelligence coverage through curating and de-duplicating the data in these feeds, which is certainly a consideration for enterprises that have been collecting feeds and don't know when they've gotten enough.

**Competition**

There are several close competitors in the areas of threat intelligence aggregation, analysis and sharing. Cyveillance had been working on a marketplace of its own, but then focused on bringing out its SMB-friendly Social Media Watch platform, along with its recently unveiled Cyber Threat Center with many tools and resources for analysts. (Interestingly enough, the one case study on ThreatStream's website is that of one of the QinetiQ branches. Before it was acquired by VenCore, QinetiQ North America was the parent company of Cyveillance; now Cyveillance reports to QinetiQ.
Cisco’s ThreatGRID, Cyber Squared’s ThreatConnect, IID, Red Sky Alliance, FireEye, AlienVault, CyberIQ Services and Vorstack all offer platforms for sharing threat intelligence. ThreatStream hopes to co-opt many other vendors that don’t (yet) have a collaboration platform: Norse, CrowdStrike, Emerging Threats, iSIGHT Partners, Webroot, Verisign iDefense, ThreatTrack, Seculert, AnubisNetworks, Malcovery, Lookingglass, BitSight, Websense, and others. The big portfolio companies, such as HP, Dell, IBM, Intel-McAfee, Symantec and Trend Micro, aren’t likely to add an external-facing collaboration offering that would mix non-customers with their own customers - that would muddy the waters. The same goes for MSSPs.

**SWOT Analysis**

**Strengths**
With its ArcSight pedigree, ThreatStream knows how to make threat intelligence data digestible to SIEMs. It’s bringing out differentiators, such as the Modern Honey Network and its threat intelligence APP store, to keep the innovation going.

**Weaknesses**
If anything can be said to be working against ThreatStream, it’s youth: it has the ArcSight pedigree, but that may not be enough to help it prevail in newer areas such as collaboration, where it has to collect members as quickly as possible in what will probably turn out in the long run to be a zero-sum game.

**Opportunities**
The ‘center of gravity’ for commercial threat intelligence collaboration is still up for grabs. Although there are many challenges inherent in threat intelligence sharing (see our recent long-format report), ThreatStream stands as good a chance as any to grab that brass ring.

**Threats**
Nearly all of the players in the threat intelligence and analytics markets are trying to become the top layer or broker for everyone else. In this ‘race to the top,’ ThreatStream has to beat some more established rivals that have been around longer. Unless it can become the platform of choice for the industry’s Information Sharing and Analysis Centers, it might end up competing with them as well.