Data Sheet

ThreatStream Integrator™

Bridging the gap between your STIX/TAXII repository and your security infrastructure

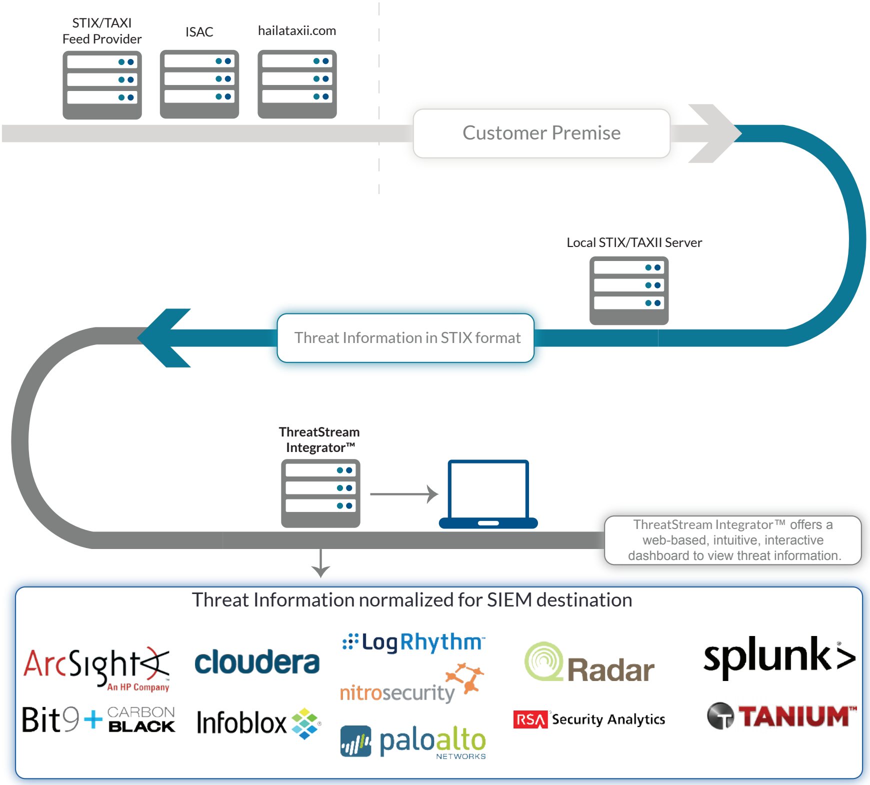
The Problem: No way to easily operationalize STIX/TAXII-compliant threat information across your security infrastructure

SOC operators, CSIRT teams, and security analysts and researchers are in a race against time. The good news is that there's an overwhelming amount of "threat intelligence" available today. The bad news is that it takes a long time to consume and operationalize this intelligence across your security infrastructure.

If your organization is part of an Information Sharing and Analysis Center or Organization – an ISAC or an ISAO – much of the threat intelligence you're consuming is probably based on the STIX/TAXII standards for describing and exchanging cyber threat information. Many ISACs, such as the Financial Services ISAC (FS-ISAC), rely on a STIX/TAXII repository to facilitate threat information sharing across the members of their trusted communities. Standards-based or not, this threat intelligence is still difficult to integrate with other security products essential to protecting an organization. The process is manual and error-prone.

The Solution: ThreatStream Integrator™, which provides the essential connection from STIX/TAXII-compliant sources to security products and solutions that can operationally leverage this intelligence

ThreatStream Integrator™ provides the essential connection that security and incident response teams need to translate raw STIX/TAXII data into usable intelligence: It integrates any STIX/TAXII repository with your security infrastructure.



ANOMALI™

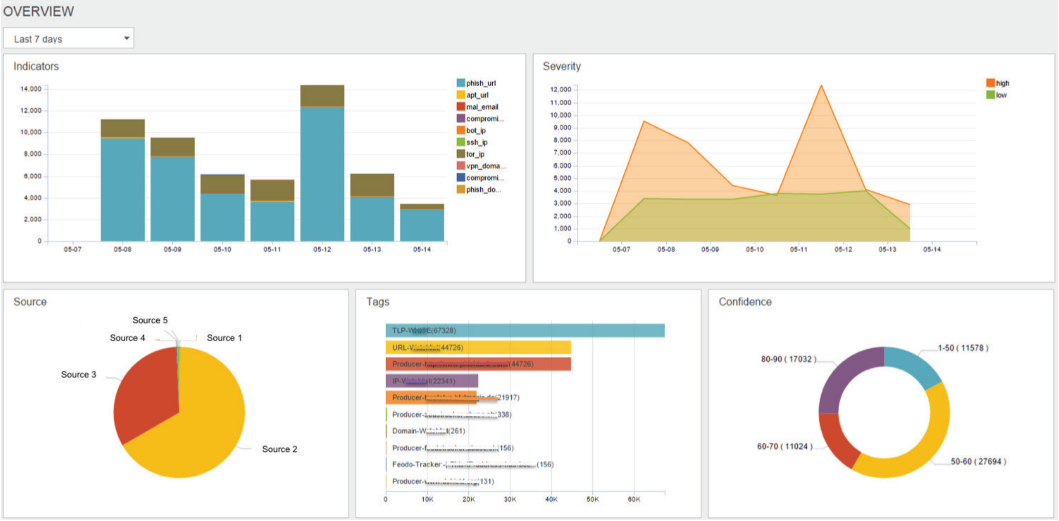
ANML-DS-TS-022216-01

Data Sheet

ThreatStream Integrator™

Anomali also offers ThreatStream 6.0, the first threat intelligence platform that manages the entire life-cycle of threat intelligence, from multi-source acquisition to operational integration across the entire eco-system of existing security devices. ThreatStream 6.0 enables enterprises and government organizations to seamlessly aggregate and analyze threat intelligence and automatically integrate the information into their security infrastructure and controls.

ThreatStream Integrator™ can connect to any STIX/TAXII server in the cloud (for example, http://hailataxii.com or a server hosted by an ISAC), or on premise, and pull threat information from it into existing security solutions – including HP ArcSight ESM and Splunk – in a format appropriate for that solution. An instance of ThreatStream Integrator™ can retrieve threat information from multiple sources and forward it to multiple destinations in an organization's infrastructure. The Integrator™ has easy-to-use, interactive dashboards enable threat intelligence visualization, deeper analysis, and advanced searches.



Key Features

Optimized to work with ISAC communities and raw IOC aggregators

- Translate raw STIX/TAXII data into formats that HP ArcSight ESM and Splunk can understand; many more integrations to come
- Easy-to-use interface to view threat information received through STIX/TAXII feeds
- Ability to run a keyword search to look for a specific indicator, search for an indicator type over a time range of your choice, and drill-down on specific indicator matches for details

System Requirements

ThreatStream Integrator™ is a lightweight application currently supported on Linux (64-bit), using any RedHat, CentOS, and Ubuntu release running Linux kernel version 2.6 or later, and SUSE Enterprise 12.

ANML-DS-INTG-022216-01