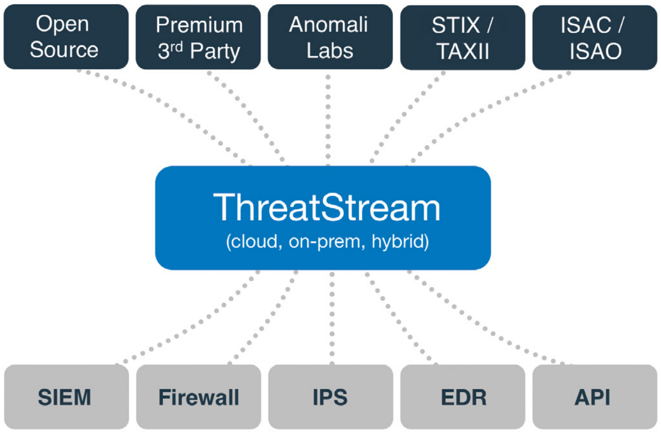
ANOMALI®

ThreatStream®

The Most Widely Adopted Threat Intelligence Platform

Threat Intelligence Overload

SOC analysts, incident response teams and researchers face the challenge of operationalizing an overwhelming amount of threat data. A recent Ponemon survey showed that 78% say threat intelligence is critical for achieving a strong security posture but also showed that 70% are overwhelmed with threat data. Anomali ThreatStream® makes it easier for security teams to achieve the full promise of threat intelligence. ThreatStream automates all the processes for collecting, managing and integrating threat intelligence, and gives security analysts the tools and resources to respond quickly to active threats.



Get the Ponemon study:
State of Threat Intelligence:
anomali.com/ponemon

Collect

ThreatStream manages ingesting intelligence from many disparate sources, including:

- STIX/TAXII feeds
- Open source threat feeds
- Commercial threat intelligence providers
- Unstructured intelligence: PDFs, CSVs, emails
- ISAC/ISAO shared threat intelligence

Manage

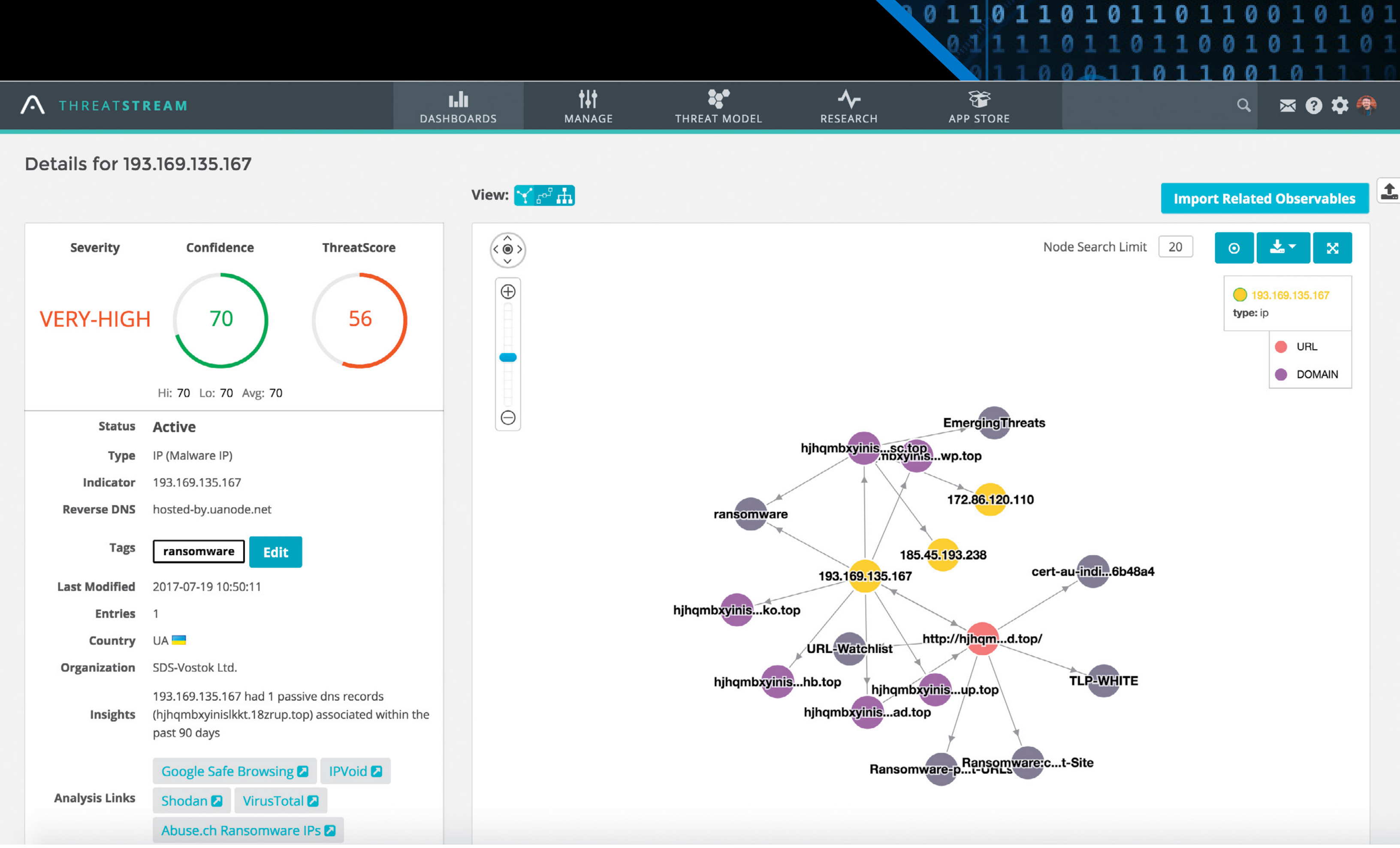
ThreatStream takes raw threat data and turns it into rich, usable intelligence:

- Normalizes feeds into a common taxonomy
- De-duplicates data across feeds
- Removes false positives
- Enriches data with actor, campaign, and TTP
- Associates related threat indicators

Integrate

ThreatStream integrates with internal security systems to make threat intelligence actionable.

- Deep integration with SIEM, FW, IPS, and EDR
- Scales to process millions of indicators
- Risk ranks threats via machine learning
- Includes Threat Bulletins from Anomali Labs
- Secure, 2-way sharing with Trusted Circles



Details for 193.169.135.167

Severity	Confidence	ThreatScore
VERY-HIGH	70	56

Hi: 70 Lo: 70 Avg: 70

Status	Active
Type	IP (Malware IP)
Indicator	193.169.135.167
Reverse DNS	hosted-by.uanode.net
Tags	ransomware
Last Modified	2017-07-19 10:50:11
Entries	1
Country	UA
Organization	SDS-Vostok Ltd.
Insights	193.169.135.167 had 1 passive dns records (hjhqmbxyinislkkt.18zrup.top) associated within the past 90 days
Analysis Links	Google Safe Browsing IPVoid Shodan VirusTotal Abuse.ch Ransomware IPs

Enabling the Analyst

Anomali ThreatStream provides tools to make analysts more efficient and increase the effectiveness of their use of threat intelligence. The ThreatStream platform includes analyst-friendly features such as:

- Malicious file examination via a built-in sandbox
- Association of indicators to cyber Actors
- Contextual data: WHOIS, PassiveDNS, others
- Threat investigation engine with analyst workflows
- Easily produce and share threat intelligence
- Brand monitoring: detection of brand abuse
- Collaborate with peers via Trusted Circles

ThreatStream Advantages

ThreatStream speeds detection and response time by operationalizing threat intelligence and uniting your security tools under one platform.

- Centralizes all your threat intel data in one place
- Turns raw indicators into actionable intelligence
- Integrates with existing security investments
- Accelerates incident response time
- Makes security analysts more efficient

To find out more about Anomali ThreatStream visit www.anomali.com/threatstream or contact info@anomali.com.

ANOMALI®