

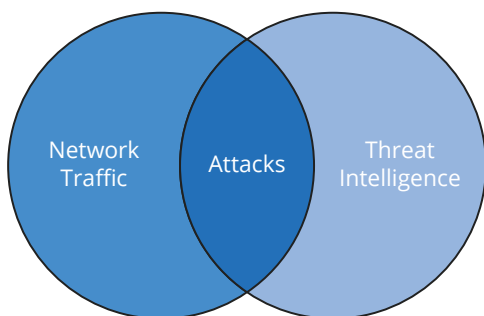
Anomali and Recorded Future Integration Dramatically Advances Your Threat and Security Operations

Anomali ThreatStream and Recorded Future Integration

Recorded Future for Anomali ThreatStream allows organizations to quickly resolve security threats using external threat intelligence and rich context from Recorded Future directly on top of ThreatStream data. Analysts are able to view related risk and evidence assigned to IPs, Domains, Hashes, and URLs through the enrichment application. Full transparency is provided on the evidence applicable to any given IOC (indicator of compromise). Additionally, risky IOCs are grouped together and used to correlate against suspect observables on your network.

Using Recorded Future risk list feeds, analysts are able to correlate against high fidelity datasets from Recorded Future as a source within ThreatStream. Recorded Future risk rules are mapped to ThreatStream iTypes for use within security controls to stop threats faster.

As a result, security and threat analysts can make quick and effective decisions at critical moments.



Anomali ThreatStream aggregates threat intelligence under one platform, providing an integrated set of tools to support fast, efficient investigations, and delivering “operationalized” threat intelligence into security controls at machine speed. Additionally, ThreatStream accelerates the process of collecting all of your global threat data into a single high-fidelity set of threat intelligence.

Joint Solution

Aggregating multiple sources of threat intelligence data into a single place can be time-consuming and manual. Ensuring the data being aggregated is valuable requires laborious validation. The integration between Recorded Future and Anomali ThreatStream provides a seamless way to bring high fidelity datasets from Recorded Future’s comprehensive breadth of sources into ThreatStream for rapid insights and streamlined investigation.

Recorded Future enrichment inside ThreatStream delivers full transparency of the riskscore and risk assigned to IOCs.

The joint solution enables analysts to instantly integrate prioritized and actionable threat intelligence with your existing security controls and technology.

The screenshot displays the Anomali ThreatStream interface. At the top, there are navigation tabs: DASHBOARDS, MANAGE, THREAT MODEL, RESEARCH, and APP STORE. Below this is a 'Settings' section with various configuration options. The main area shows a network graph with nodes and connections. A 'Recorded Future' widget is overlaid on the graph, displaying a 'DEACTIVATE' button. Another widget shows a risk score of 69 for IP address 222.186.21.166, with a 'Malicious' status and a risk score of 89. Below these are 'Enrichments' for 'PASSIVE DNS (7)', 'RECORDED FUTURE', and 'WHOIS'. A 'Summary' table is visible at the bottom, with columns for Risk Score, Criticality, References, Date First, Date Last, and Link. The table contains one row with a risk score of 24 and a link to a Recorded Future entry.

Risk Score	Criticality	References	Date First	Date Last	Link
24	Unusual	851	2015-04-14 22:05:42	2017-04-27 22:13:25	https://www.recordedfuture.com/feeds/entry/ip:222.186.21.166

Use Cases


The integration between Anomali ThreatStream and Recorded Future allows security responders to:

- Detect and gain context on IOCs with real-time external intelligence to identify true incidents and dismiss false positives using the enrichment application
- Proactively block threats before they impact the business using the Recorded Future risk lists
- Reduce time for threat detection, remediation, and response



About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

 www.recordedfuture.com  [@RecordedFuture](https://twitter.com/RecordedFuture)

© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.



About Anomali

The Anomali suite of threat intelligence solutions empowers organizations to detect, investigate and respond to active cybersecurity threats. The award-winning ThreatStream threat intelligence platform aggregates and optimizes millions of threat indicators, creating a "cyber no-fly list." Anomali integrates with internal infrastructure to identify new attacks, searches forensically over the past year to discover existing breaches, and enables security teams to quickly understand and contain threats. Anomali also offers STAXX, a free tool to collect and share threat intelligence, and provides a free, out of the box intelligence feed, Anomali Limo.

To learn more, visit www.anomali.com and follow us on Twitter: [@anomali](https://twitter.com/anomali).