PARTNER DATASHEET

TEAM CYMRU

ANOMALI

Transform your cyber defenses with real-time actionable threat intelligence

Make informed security decisions with unmatched agility and precision

Seamlessly merge Anomali's resource visibility and SOC productivity tools with Team Cymru's unrivalled threat intelligence

Gain rich context across internal telemetry and external threats

Using integration and automation, Anomali supports the processing of extracted malware samples from Team Cymru into its Match Threat Detection system

Enhanced SIEM Platform Efficiency

With the integration of Team Cymru's hourly updated threat feeds into SIEM platforms, organizations gain the ability to correlate events, enhance accuracy of threat detection and significantly reduces false positives

Pure Signal ™

FEEDS

What are Threat Feeds

Raw threat feed data that can be integrated directly into automated workflows adding rich context to enable Network Security Teams, Threat Researchers & Hunters, and Malware Analysts to scale and accelerate.

How it works

Hourly-generated structured XML files provide a 24-hour retrospective view of all observed malicious events. When integrated with SIEM, SOAR, and defense solutions, they enable real-time alerts, continuous monitoring, and the implementation of proactive defense measures.

Tailored Threat Intelligence

The feeds are customized to meet the distinct requirements of SOC and Research teams. They provide specialized insights into Botnet Analysis & Reporting (BARS), Command and Control (C2) infrastructures, and IP Reputation, ensuring that each team receives relevant and actionable intelligence for their specific needs.

GET STARTED

anomali.com/marketplace/threat-intelligence-feeds

Our joint solution synergizes Team Cymru's robust threat feeds with Anomali's ThreatStream innovative capabilities to transform raw data into actionable threat intelligence.

This integration boosts SIEM platform efficiency, enabling better event correlation and reduces false positives.

Together, we empower organizations to proactively tackle emerging cyber threats with greater accuracy and speed.

Botnet Analysis & Reporting (BARS)

Provides a holistic view of adversarial campaigns.

Key Facts:

In-depth analysis tracking and history of malware families that utilize unique control protocols and encryption mechanisms. Updated every 60 minutes for near-real-time global Internet visibility of C2 and DDoS attacks.

Use Cases:

Monitor and mitigate sophisticated malware attacks targeting your network, track cyber espionage campaigns, and protect infrastructure from DDoS attacks and complex malware.

450k+

Unique IPs Daily

30-50M

Daily Events

Controller Feed (C2)

For blocking compromised nodes, malicious attachments, and enhanced firewalling.

Key Facts:

Real-time identification of botnet command and control (C2) IPs, continuous monitoring of inactive nodes and networks. Includes all possible IP addresses, domain name, HTTP URL, first seen time, and confidence score.

Use Cases:

Block traffic to known malicious controllers, integrate into IDS to enhance their security, or utilize the feed for proactive security measures, preventing malicious traffic from affecting networks.

40k+

Unique IPs Daily

40+

Malware Families

IP Reputation Feed

Provides IP centric lighter weight feed of controller and victim IPs.

Key Facts:

Lightweight, near-real-time feed of all controllers and victims.
Offers visibility into botnets that normally evade monitoring.
Includes categories of compromised devices like routers, darknet visitors, & abused proxies.

Use Cases:

Block traffic from compromised IP addresses, reduce fraud, secure client data transmission, and maintain online gaming fair play by blocking connections from known malicious IPs.

90k+

Unique IPs Daily

150+

Tracked Botnets

About Team Cymru

TEAM CYMRU

Team Cymru's mission is to save and improve human lives. We are unrivalled across three disciplines; digital business risk platforms, free-to-use community services, and support services to over 143 Government CSIRT teams.

Our business risk and threat intelligence platforms empower global organizations with unmatched Threat Reconnaissance and Attack Surface Management capabilities to meet the challenges of today's cyber threats.

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.

ANOMALI