Product Guide

PURE SIGNAL™
FEEDS

Empower SOC, IR, Defense & Research teams with the most comprehensive threat feeds available

☑ ***Real-Time Data for Proactive Security.*** *With real-time updates every hour, our threat feeds equip you with the latest intelligence, enabling swift responses to emerging and evolving cyber threats.*

☑ ***Extensive Global Data Enhances Detection.*** *Our feeds draw from an extensive network of global data sources, providing comprehensive threat insights that enhance detection and improve your defenses.*

☑ ***Collaborative Intelligence for Robust Defense.*** *Leveraging a collaborative model with global partners, our threat feeds offer enriched data, amplifying your capability to anticipate and mitigate cyber threats effectively.*

Automate your cyber defenses

REAL-TIME THREAT INTELLIGENCE THAT CREATES BETTER DEFENSE

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.

SIGN UP HERE
www.team-cymru.com

Contact your Pure Signal™ Feeds Representative directly:

sales@cymru.com

TEAM CYMRU

PURE SIGNAL™

FEEDS

Transform your defenses with the most accurate threat feeds available

- ☑ Discover or mitigate malware that detection tools have missed
- ☑ Block malicious communications and prevent payload execution
- ☑ Gain visibility into botnets that normally evade monitoring

Botnet Analysis & Reporting (BARS)

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.

450k+
Unique IPs Daily

30-50M
Daily Events

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

Controller Feed (C2)

40k+
Unique IPs Daily

40+
Maware Families

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.

IP Reputation Feed

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.

90k+
Unique IPs Daily

150+
Tracked Botnets

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.

About Team Cymru
Our 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. www.team-cymru.com