
TEAM CYMRU™
PURE SIGNAL
DISCOVER THE WORLD'S LARGEST
IP INTELLIGENCE DATA OCEAN

ABOUT PURE SIGNAL

The biggest advantage in the fight against cyber crime

TEAM CYMRU

Trusted by Those You Trust

For over 25 years, Team Cymru has been a leader at empowering governments, law enforcement agencies, and militaries to detect and defend against the most sophisticated nation-state threats, illegal activities, and malicious networks.

In the hands of the private sector, our unique capabilities provide unparalleled visibility into cybercriminal activities, victims, and advanced persistent threats across the internet. With Pure Signal, our customers gain the ability to discover, defend, remediate and recover from cyber attacks faster than ever before.

Unmatched Size & Scale of Threat and Risk Data

Every day, our platform analyzes over 300 billion IP to IP communications, setting a new standard in threat intelligence volume and depth. As the largest provider of intelligence at this scale, we serve as a force multiplier for analysts, equipping them with the tools to effectively combat attacks and mitigate risks.

Real-time Insights

Unlike static reports and other data sources, the Pure Signal Platform delivers uncurated, real-time, actionable insights for global IP intelligence. This enables Incident Response and Threat Hunting teams to operate with the highest fidelity and quality insights available, empowering them to stay ahead of evolving threats.

Depth & Breadth

Team Cymru offers over 40 datasets unmatched in scale, and extends its services to provide up to 90 days of historical data. This breadth of coverage ensures that our customers have access to comprehensive insights into cyber threats and vulnerabilities.

Accuracy

Our customers trust us because we deliver the highest quality data with stringent validation processes. With over 20 years of experience curating our IP intelligence data ocean, we combine automated algorithms with human expertise to ensure unparalleled accuracy. Our commitment to precision sets us apart, providing our customers with the confidence they need to make informed decisions in their cybersecurity strategies.

300bn+

IP communications analyzed

Every Day

Unique community-led collaboration of over 1,000 ISPs and network operators

A data ocean that can be accessed in real time across a variety of platforms

40+

Datasets with up to 90 days history to search and query

USE CASE

Supply Chain Risks and Threats

Continuous Monitoring of Compromise across the Supply Chain

Our Threat and Risk platforms help illuminate compromised supply chain partners, and are the game changer for organizations seeking to reduce operational risks from third parties.

> *"We were able to flesh out third-party infrastructure, monitor it for signs that they might have been compromised, and in many cases, we knew that they'd been compromised before our partners knew."*
>
> Threat Intelligence Manager, UK Retail Bank

Without continuous exposure management across company assets and third party infrastructures, organizations are left wide open to the risks and threats from the weakest link in the chain.

Raise the Cost of Attack for Persistent and Repeat Attackers

Criminals and threat actors will probe for weak links across your systems and supply chain partners to exploit them. They will repeat attacks until they have exploited every unpatched vulnerability and explored every way to gain access to critical financial, operational or customer-facing systems that provide access to customer information.

> *"We found great utility in being able to preemptively stop an attack with visibility into changes that threat actors were making to their infrastructure in an effort to attack us again."*
>
> Threat Intelligence Manager, UK Retail Bank

Our Threat and Risk Platforms provide continuous and autonomous discovery of third party assets and vulnerabilities. Analysts are enabled to create automated queries that provide near real time insights - the key advantage when facing down fast moving adversaries and evolving third party infrastructure.

React Faster and Anticipate Attacks

You know your internal systems, services, infrastructures and networks, but threat actors have visibility of your external facing assets. Our Pure Signal products ensure your visibility of the threat actors' infrastructure is unmatched. When you gain visibility of an attacker's own assets and infrastructure, you can start to create proactive security strategies so analysts react faster and can start to anticipate attacks.

> *"Recon has allowed us to pay more attention to the [bad] actors instead of reading reports about [them]. It has allowed us to create our own intelligence, monitor our stuff better, and react to things much faster."*
>
> Lead security analyst, Global retail organization

Faster discovery, incident response and recovery are mission critical. Every minute of impact or distraction results in lost dollars and productivity. Team Cymru Threat and Risk platforms elevate every cyber security team to flatten time to discover, respond and solve the most challenging cyber threats you face.

USE CASE

Ransomware

TEAM CYMRU

Ransomware Disrupts your Entire Supply Chain

Identifying compromised organizations across the supply chain or your own infrastructure is the difference between headlines and bottom lines. The insight and visibility you need are simply not possible with curated or finished threat intelligence.

> *"The worst part when thinking about supply chain security is the software supply chain compromise which is just a horror show, and when you look at all the news that comes out every day, it's turning into more of a horror show by the moment."*
>
> Analyst, Large Retail Bank

Being reactive is no longer an option for the digital age, allowing threat actors to infiltrate your networks, and disrupt with profit-draining ransomware drain. Team Cymru's threat platforms provide the most complete and expansive visibility of your threats and the risks that relate to your organization.

Mitigating Repeat Ransomware Attackers

Your missing strategic advantage is not knowing your adversary and their infrastructure as you do your own, and being unaware when your supply chain is compromised. Evasive code used by your adversaries can linger for months before starting outbound communications that are missed by your security technologies.

> *"...we saw a major increase in ransomware hitting our third parties. If they are compromised in any way, shape, or form, then our IR and legal teams become actively involved. They make sure that no data related to us is leaked, that [the third party's] network is secure and that [the third party] won't be used as a pivot to get into our networks."*
>
> Lead Analyst, Fortune 100 Organization

Team Cymru threat platforms provide the visibility your teams need to ensure no lingering attacker malware or code is beaconing out to malicious infrastructure - a signal of continuous infection.

Anticipating Ransomware Attacks

Yesterday's threat intelligence is stale and not useful to make effective decisions today. Reliance on third-party generated and curated threat intelligence only provides vague and generic information about threats that may, or may not, directly impact your organization. Analysts waste time on stale threat intelligence, then it is discarded.

> *"With Recon, we map the infrastructure being used by some ransomware groups. We block them from entering our network, monitor their infrastructures as they evolve, and monitor potential victims such as third-party entities. When [a third party is] compromised, we identify it with Recon, then tell [the third party] how [the threat actor] got in ... and what they need to do to stop them immediately."*
>
> Lead security analyst, Global Retailer

Our threat platforms put you in control of the knowledge you need to make agile and effective decisions, that ultimately lead to longer lasting outcomes. Without curation or finished reports, your teams directly access the information that gives you the advantage: nowhere to hide for your most persistent Ransomware adversaries.

USE CASE
Phishing

Reduce operational costs and Improve blocking

Phishing continues to be profitable for criminals, and is one of the largest sources of revenue for the underground economy. Attempts to steal credentials from your organization to sell or gain access using Phishing techniques are not going to stop anytime soon. Yet regardless how effective your team is at combatting this frustrating cyber challenge, or how good block lists are, there are ways of gaining efficiencies and adding more value to the organization.

> ***"We have multiple processes that update the block list, but with what we glean from Recon, we have been able to go from 15 feeds to five feeds."***
>
> Lead security analyst, Global Retailer

Our Threat and Risk Platforms allow organizations to significantly reduce data sources to reduce cost and complexity of combatting Phishing. This enables your organization to gain from improved information used for automating block-list updates as threat actors update their Phishing infrastructures.

Accelerate Incident Response

During a Phishing attack there is a frenzy of activity. But what about ensuring the threat actor can't reach their intended goals or objectives?

> ***"A key component of the Recon feed is that if threat actors get in, it doesn't mean that they can get anything out."***
>
> Lead Analyst, Fortune 100 Organization

Team Cymru's Threat Platforms inform how to improve perimeter defenses and block outbound traffic to known threat actor infrastructure, or compromised IP space known for Phishing.

Validate Clean-up and Recovery

One remaining compromised device still beaconing to C2 infrastructure is all it takes to reset the cyber attack cycle. The aftermath of any cyber attack is costly, and that long tail only gets more expensive.

Ensure no lingering attacker malware or code is beaconing out to their infrastructure.

THREAT INTELLIGENCE

TEAM CYMRU

RECON

Recon is a web-based threat intelligence tool for advanced security analysts and mature SOC Teams.

With a simple GUI, graphical displays, tagged results and powerful query tools, it transforms how sophisticated users hunt, assess, and monitor advanced persistent threat actors.

It is the place to greatly enhance investigations for single IPs, domains, or entire CIDR ranges related to malicious activity.

USE CASES

☑ **Supply Chain Security**
Real-time detection of threats within partner networks to prevent breaches.

☑ **Repeat Attacker Defense**
Identify and monitor evolving threats to protect against persistent attackers.

☑ **Data Breach Prevention**
Proactively block new threats outside your perimeter, reducing risk.

SCOUT

Scout Ultimate is a web-based threat intelligence tool for security analysts of all experience levels.

With a simple GUI, graphical displays, tagged results, and easy to use searches, it helps quickly determine if suspicious IPs are malicious or compromised.

It is the place to start investigations for single IPs, domains, or entire CIDR ranges related to malicious activity.

USE CASES

☑ **Streamline Incident Response**
Consolidate tools and reduce alert fatigue for SOC analysts and investigate suspicious IPs In real-time to drastically reduce false positives. Senior analysts can make informed assessments, and IR teams receive real-time intelligence for defense updates.

☑ **Create Actionable Threat Intelligence**
Keep up with evolving threat actor infrastructure and attack campaign changes. Support updating of defense policies to proactively mitigate targeted attacks.

☑ **Automate Security Workflows**
Leverage integrations to optimize and enhance detection capabilities of SIEM, XDR, and SOAR tools, enabling faster incident response.

THREAT FEEDS

TEAM CYMRU™

FEEDS

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

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.

USE CASES

☑ **Discover or mitigate malware that detection tools have missed**
Real-time updates every hour.

☑ **Block malicious communications and prevent payload execution**
Our feeds draw from an extensive network of global data sources.

☑ **Gain visibility into botnets that normally evade monitoring**
Monitor and mitigate sophisticated malware attacks.

EXTERNAL DIGITAL RISKS

ORBIT

Orbit is a cloud based attack surface management platform that enables discovery, monitoring and managing of external digital risks and vulnerabilities.

Our innovations enable financial organizations to gain immediate value through visibility of hidden assets, unknown vulnerabilities and third party risks that otherwise go undetected.

Our platforms uniquely use Pure Signal, so our customers can discover up to 500% more assets compared with other providers, then gain continuous and autonomous updates on vulnerabilities, mitigate financial losses, regulatory fines, M&A issues and manage supply chain risks more effectively.

USE CASES

☑ **Shadow IT Discovery**
Autonomous discovery of assets, infrastructure and technologies across all external environments.

☑ **M&A, Third-Party Risks and Threats**
Avoid costly indirect attacks by monitoring third parties for risks, then proactively eliminate the weakest links in the security chain.

☑ **Align with Regulatory Compliance**
Inform GRC and enable IT to function harmoniously, minimize financial impact of sensitive customer data and online services being exposed.

TEAM CYMRU™

ABOUT US

Since 2005, Team Cymru's mission has been to save and improve lives.

We strive to achieve our mission by working with security teams around the world, enabling them to track and disrupt the most advanced bad actors and their infrastructures.

Through our Community Services, we deliver comprehensive visibility into global cyber threat activity and are a key source of intelligence for many cyber security and threat intelligence vendors. Our Community Services division provides no-cost threat detection and intelligence to network operators, hosting providers and more than 140 CSIRT teams across 86+ countries.

With our Commercial Solutions, we provide enterprise clients comprehensive visibility into global cyber threats & risks. Security teams rely on our Pure Signal™ platform to close detection gaps, accelerate incident response, and detect threats and vulnerabilities across their entire enterprise and third-party ecosystems. www.team-cymru.com

CONTACT
tel: +1 847-378-3300
sales@cymru.com