# No-Cost
## and Commercial Solutions

TEAM CYMRU

# Pure Signal™ RECON

## If your visibility ends at your enterprise perimeter, how do you get ahead of critical threats?

The cybersecurity industry has come to accept the concept of "threat hunting" as searching for indicators of compromise within the enterprise. However, if you discover IOCs within your enterprise, that is no longer a threat. It's a reality.

Talk to us about the value of external threat hunting with our commercial offering, **Pure Signal™ Recon.** Learn how many organizations are turning the tables on their adversaries.

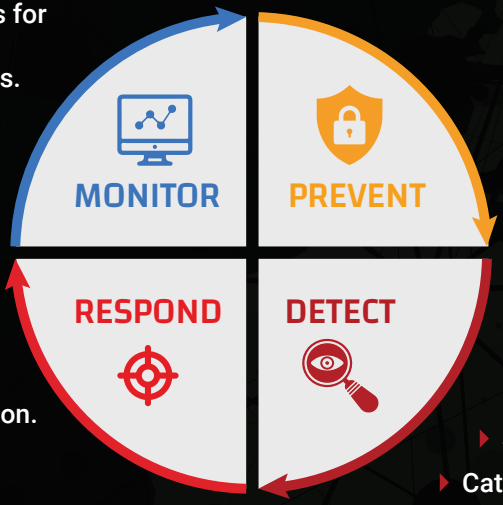
> "We were able to see the infrastructure stood up before the phishing emails even went out."
>
> - Lead Analyst, Fortune 100 Institution

- Stop relying solely on outdated, piecemeal threat reports and feeds.
- Map adversary infrastructure.
- Block attacks before they're launched.
- Detect threats across your supply chain.
- Optimize root cause analysis, compromise assessment and remediation.

THE POWER OF

## Pure Signal™

- Trace, map and monitor cyber threat infrastructures across the globe.
- Monitor third-party vendors for compromises, probing and outdated operating systems.
- See when others are being attacked and use that intel to defend yourself.




- Identify and block threats before they even reach your door.
- Reduce SOC noise, prioritize alerts, fine tune alerting rules.
- Accelerate compromise assessment.
- See vulnerability probing.
- Catch threats other tools miss.
- Reduce down-time.
- Ensure comprehensive remediation.
- Prevent recurrence.



sales@cymru.com

# Nimbus Threat Monitor

## Many companies pay for our IP Reputation data.

### Nimbus partners don't.

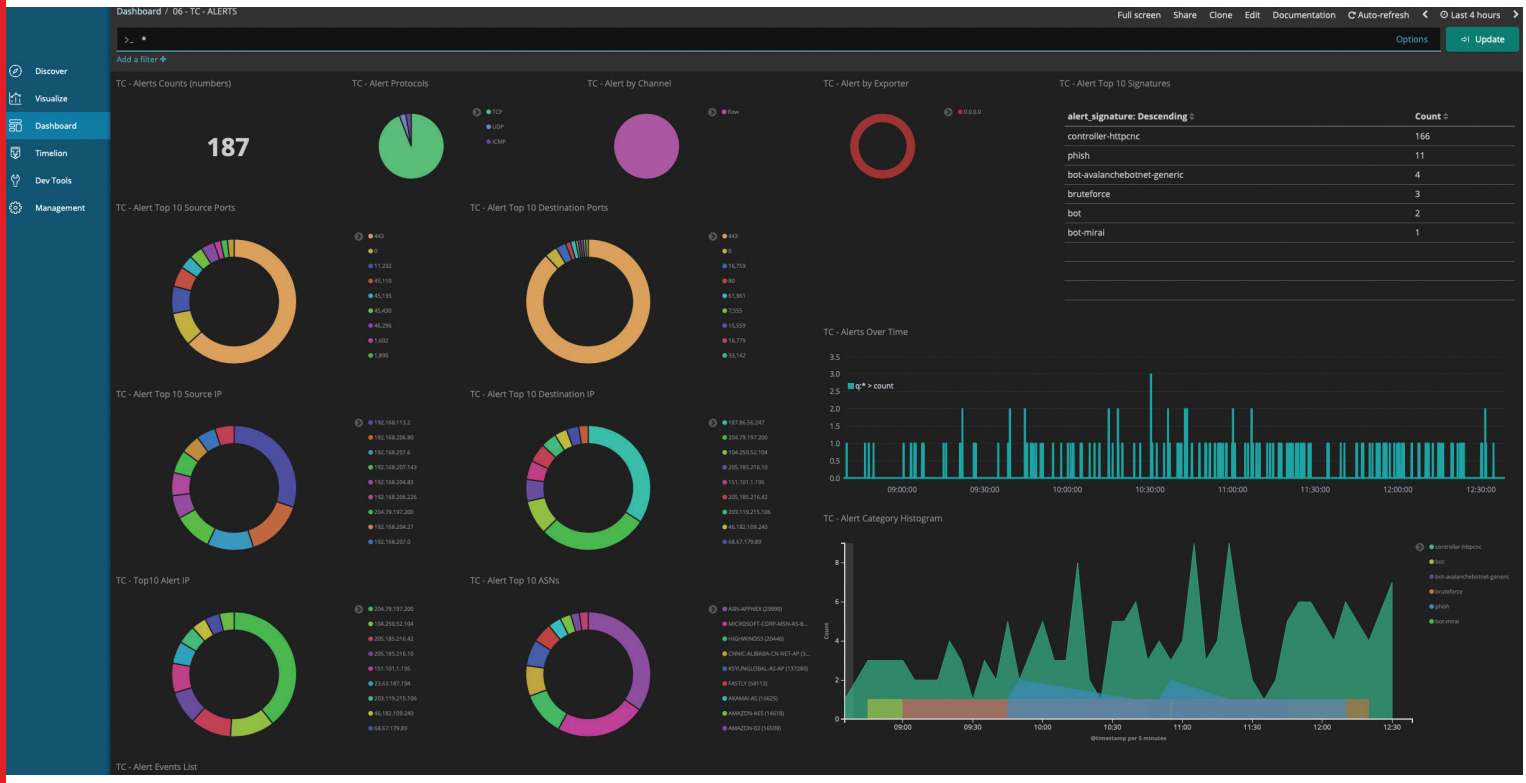
By joining us in making the internet a safer place, you will receive a purpose-built threat detection solution, created to auto-correlate your network flows with the same IP reputation data that powers many well-known cyber security solutions.

- Quickly identify compromised assets in near-real time.
- See who is draining your bandwidth for malicious purposes.
- Easily prioritize your remediation efforts while keeping the Internet safer.
- Protect your clients.
- Near-real-time threat detection.

> **"The Nimbus tool is unique and essential to our CSIRT, because it gives us a detailed view of malicious activity (botnets, controllers) on our backbone."**
>
> **– Francisco Badaró, Telecommunications and Training Manager, ITS Brasil**

- Isolate malicious activity by type, network address ranges and more.
  - –18 alert filters
  - –31 network statistics filters
- At-a-glance view of your top cyber threats and associated details.
- A daily report informs your remediation priorities.

## Talk to us about becoming a Nimbus partner.






sales@cymru.com

# Unwanted Traffic Removal Service (UTRS) 2.0

**UTRS is a global collaborative system** that helps stop large infrastructure attacks by leveraging an existing network of cooperating BGP speakers such as ISPs, hosting providers and educational institutions. The system automatically distributes verified BGP-based filter rules from victim to cooperating networks.

## UTRS 2.0 dramatically improves this service for our collaborators...

### UTRS VERSION 1

| FEATURE | DESCRIPTION |
|---|---|
| **BGP based rules propagation** | This is the functional trigger |
| **IPv4 /32 advertisements supported** | This limits requests to a single address |

### WHAT'S NEW IN VERSION 2?

| FEATURE | DESCRIPTION |
|---|---|
| **FlowSpec rules** | This allows you to create rules based on ports and protocol combinations, instead of just IP addresses. This more targeted filtering lets you stop attacks while keeping a victim's services up and running. |
| **Allow IPv4 /25 and IPv6 /49 advertisements** | Allows networks to defend against carpet bombing style attacks by requesting larger portions of their address space to be blocked. |
| **IPv6 support** | Allows networks to defend against IPv6 attack traffic. |
| **Redundant peering sessions** | Prevent single points of failure in your security framework. |
| **Route Origin Authorizations (ROAs) are honored.** | Since we validate ROAs, we support BGP-triggered DDoS mitigation service providers, allowing your service providers to defend themselves and craft the most optimal rules. |

## Ask us about our other Community Services...

### CSIRT Assistance Program
We provide daily lists of compromised or abused devices for the ASNs and/or netblocks within the jurisdictions of 135+ CSIRTs. Join us now.

### Dragon News Bytes (DNB)
Join 6000+ on this private mailing list that distributes information security news and occasional TLP-Amber threat updates.

### The Bogon Reference
We provide several resources to help you filter bogons from your routers and hosts.

### Malware Hash Registry (MHR) 2.0
This lookup service cross-references your hashes with 30+ antivirus databases and 8+ years of Team Cymru malware analysis.

### IP to ASN Mapping
Map IP addresses to BGP prefixes and Autonomous System Numbers (ASNs), based on BGP feeds from our 50+ BGP peers. Updated every 4 hours.



**CONTACT US**
tel: +1 847-378-3300
fax: +1 407-878-7833
sales@cymru.com

**EMERGENCY CONTACT**
+1 847-378-3301
support@cymru.com

TEAM CYMRU