BROCHURE

# PureSignal™ RECON

TEAM CYMRU™

# RECON

## Pure Signal™ and Ground Truth for Security Teams

Despite the numerous tools and advancements in machine learning, you are likely dealing with too much SOC noise and trapped in a perpetual game of whack-a-mole when it comes to detecting and responding to cyber threats.

This is because security teams are limited to using data gathered after a threat has broken through their enterprise defenses and threat intelligence that has been curated by vendors who rely on edge devices to collect this data. Your visibility ends at your enterprise perimeter. So, there is no way to get ahead of malicious campaigns that are constantly evolving, standing up new infrastructure around the globe, and exploiting new vulnerabilities.

As a result of these limitations, the cybersecurity industry has come to accept the concept of "threat hunting" as searching for indicators of compromise within the enterprise. That is not real threat hunting. If you discover IOCs within your enterprise, that is no longer a threat. **It's a reality.**

### What does real threat hunting look like?

1. Trace malicious activity through a dozen or more proxies and VPNs to identify the origin of a cyber threat.
2. Map the malicious infrastructure globally.
3. Block it preemptively.
4. Monitor it as it evolves to defend yourself against it indefinitely.

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

- **Network Flows**
  - Flows
- **DNS Information**
  - Banners PTR
  - DNS Queries
  - NMap Reverse DNS Lookups
  - PDNS Name-to-Address Mapping
  - Flows
  - PDNS NXDomain
  - PDNS Other Records
- **APT**
  - APT Threat DNS
  - APT Threats DNSRR
  - APT Threats Hostnames
  - APT Threats IPs
  - APT Threats Malware
- **Attacks**
  - BARS Observed DDoS Attacks
  - Observed DDoS Attack Commands
- **Botnet Information**
  - BARS Botnet Controllers
  - BARS Observed Infected Victims
- **Derived Relationships**
  - DNS Derived Domains (domain search)
  - DNS Derived Domains (IP search)
  - DNS Derived IPs (domain search)
  - DNS Derived IPs (IP search)
- **Scanning and Honeypot**
  - Conpot, ICS Honeypot
  - Cowrie, SSH and Telnet Honeypot
  - Darknet
  - Dionaea, Malware Capturing Honeypot
  - Port Scan
  - Scanner
- **Traffic Information**
  - Beacons
  - Cookies
  - RDP Traffic
  - URLs
  - UserAgents



sales@cymru.com

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.


## Hunt beyond your enterprise perimeter to find, map, block and monitor malicious infrastructure across the globe...

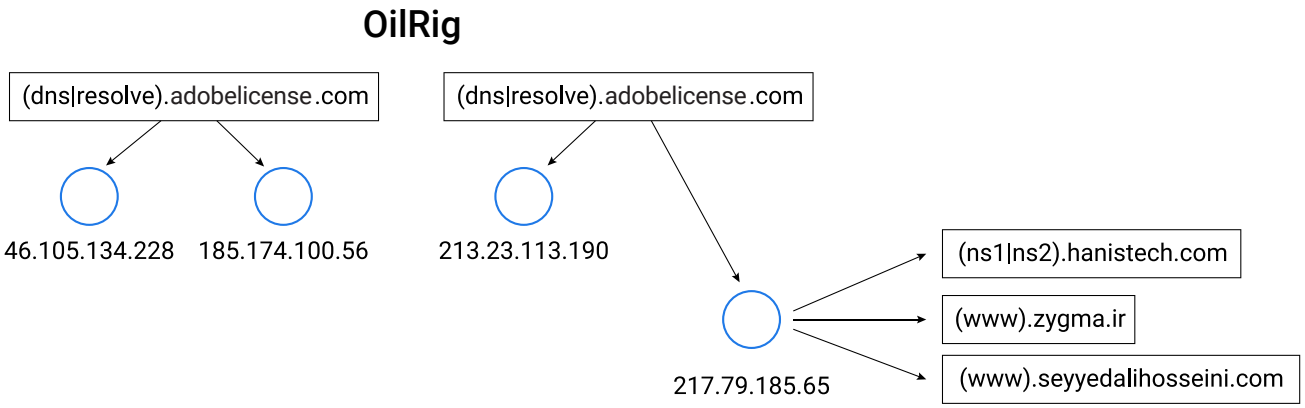
- Create targeted queries against 50+ data types.
- Employ network forensics at Internet scale.
- Track through more than a dozen hops to identify cyber threat origins.
- Correlate domains and IP addresses with malware analysis by adding Team Cymru's malware module.



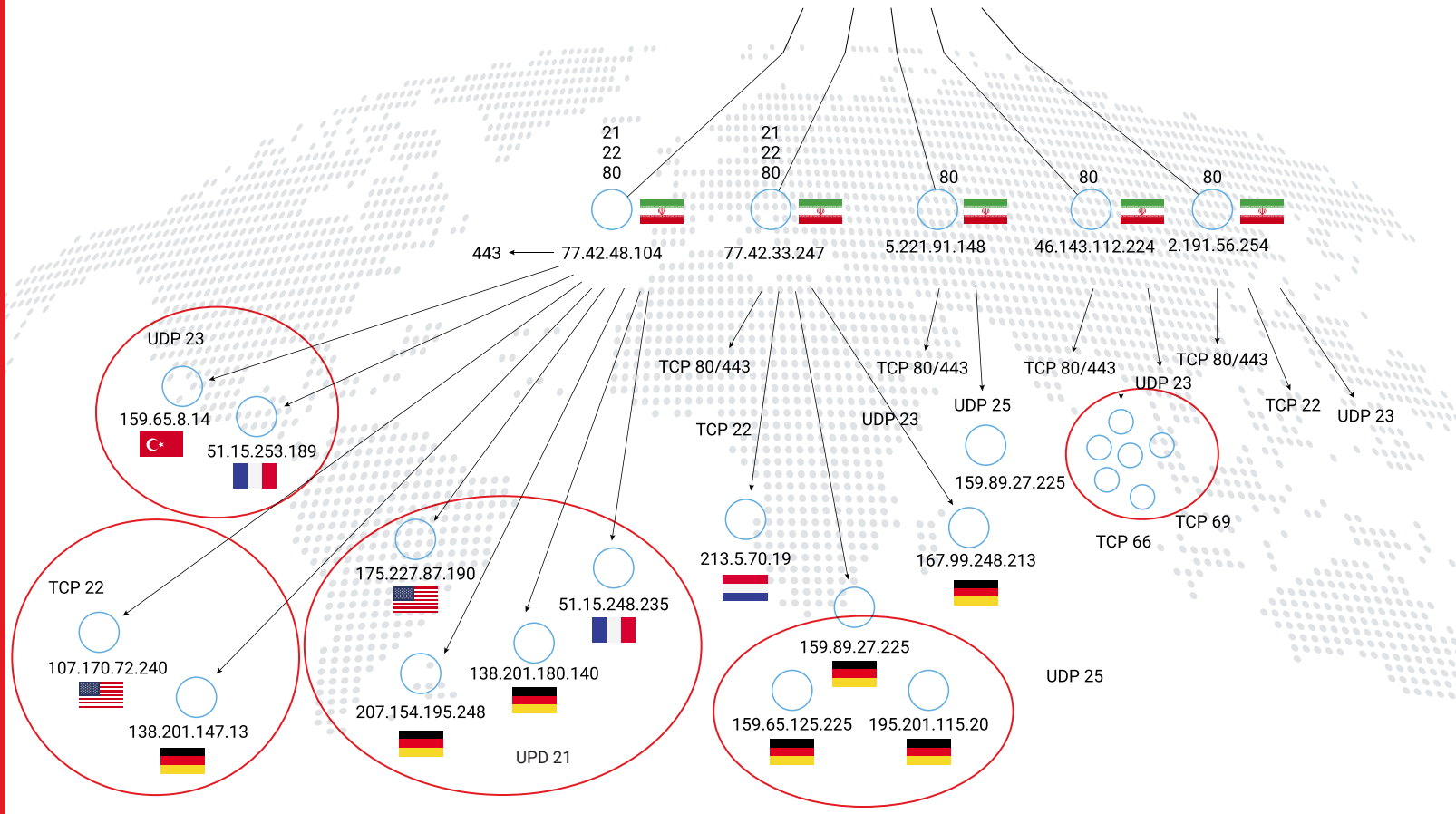
sales@cymru.com

# Map Malicious Infrastructures

## For most, visibility ends with a **few fragments** of intelligence to inform your security measures...




## ...but for those with **RECON**, visibility and insight are **global.**






**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