PureSignal™
RECON

TEAM CYMRU™

Elite teams are making external threat hunting a strategic priority.

By conducing threat reconnaissance on their high priority threat actors, mature cyber security teams are vastly improving prevention, detection, supply chain security and incident response.

The Problem

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 is fragmented and often dated.

Your actionable 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.

The Solution

Expand your network forensics capabilities to Internet scale, so you can watch threat actor infrastructures as they evolve and view your enterprise and third-party ecosystem from a threat actor's perspective. This allows you to get more out of your threat intelligence and achieve longer lasting network defense outcomes.

Minimize network and supply chain blind spots, and watch your adversaries infrastructures as they evolve.

- ⊕ Block attacks before they're launched.
- ⊕ Optimize C2 blocking.
- ⊕ Enrich your alerting rules.
- ⊕ Detect threats other tools have missed.
- ⊕ Detect supply chain threats.
- ⊕ Vastly improve incident response.

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

sales@cymru.com

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.

MONITOR

PREVENT

▶ Identify and block threats before they even reach your door.

RESPOND

DETECT

▶ Reduce SOC noise, prioritize alerts, fine tune alerting rules.

▶ Reduce down-time.

▶ Ensure comprehensive remediation.

▶ Prevent recurrence.

▶ Accelerate compromise assessment.

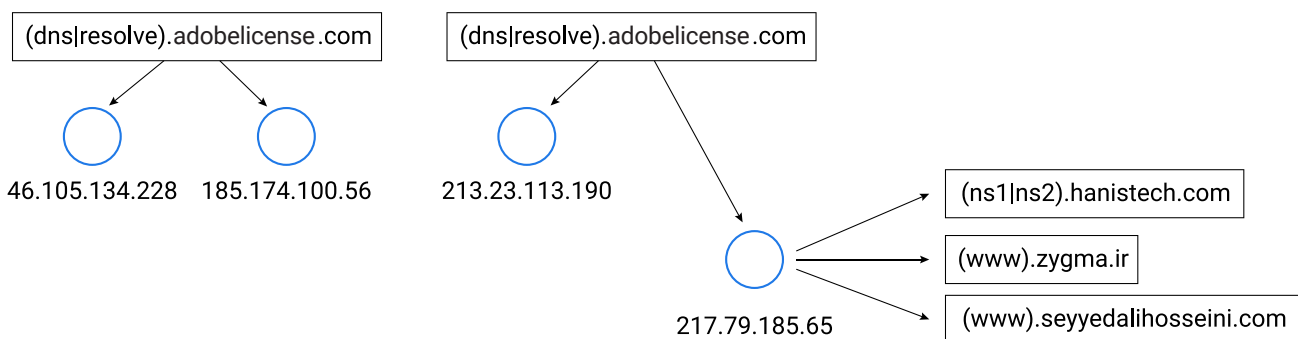▶ See vulnerability probing.

▶ Catch threats other tools miss.

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.

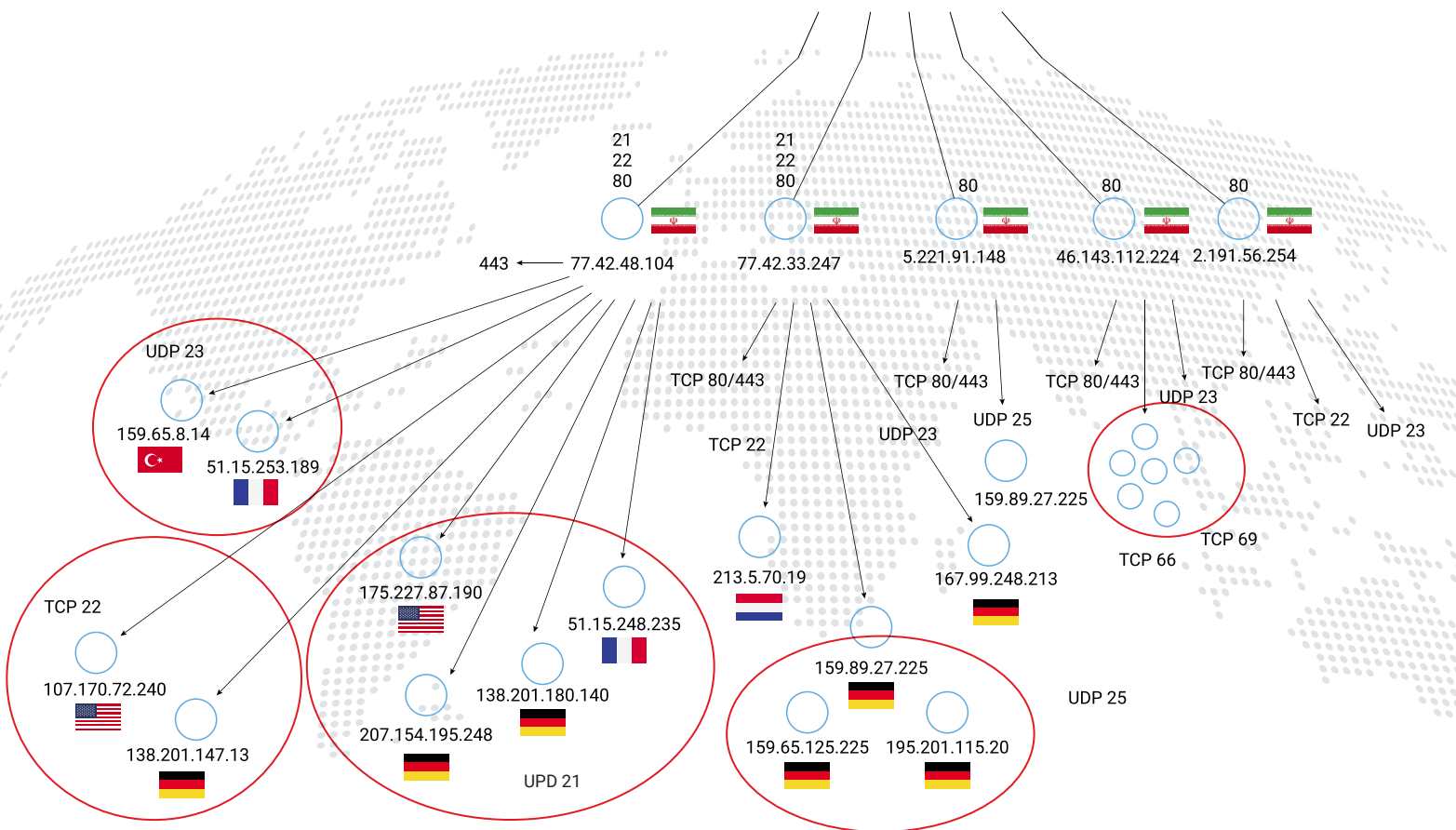- Correlate domains and IP addresses with malware analysis by adding Team Cymru's malware module.

sales@cymru.com

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

OilRig

(dns|resolve).adobelicense.com

(dns|resolve).adobelicense.com

46.105.134.228   185.174.100.56

213.23.113.190

217.79.185.65

(ns1|ns2).hanistech.com

(www).zygma.ir

(www).seyyedalihosseini.com

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

21
22
80

21
22
80

80

80

80

443 ← 77.42.48.104   77.42.33.247   5.221.91.148   46.143.112.224 2.191.56.254

UDP 23

159.65.8.14

51.15.253.189

TCP 80/443

TCP 22

TCP 80/443

UDP 23

TCP 80/443

UDP 25

TCP 80/443

UDP 23

TCP 22

UDP 23

UDP 25

159.89.27.225

TCP 69

TCP 66

TCP 22

107.170.72.240

138.201.147.13

175.227.87.190

51.15.248.235

138.201.180.140

207.154.195.248

UPD 21

213.5.70.19

167.99.248.213

159.89.27.225

159.65.125.225   195.201.115.20

UDP 25

TEAM CYMRU