Elite teams are making external threat hunting a strategic priority.

By conducting 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
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.
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.