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
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.
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**.