We collect data and build products that help our customers assess cyber threats against their network, their IP, their employees or their customers.

- **Map the Internet** at the domain and IP level
- Gather **as much data as possible** from DNS, Whois and site crawls
- **Connect** these resources to each other and to the individuals that control them.
- Enables our customers to **understand the threat level** of cyberattacks, to **profile and identify the attackers**, and to **mitigate future attacks** by the same actors.
A Brief History Lesson

**DOMAINTOOLS: FROM AD CLICKS TO FANCY BEARS**

- 2002: Earliest Data Collection
- 2008: Retail Membership Model
- 2010: Security Investigations
- 2012: Data Demand from Leading SOCs
- 2015: Iris investigative platform
- 2016: Integrations enable enrichment

Learning From The Experts

**WHOIS & DNS DATA GRANTS SECURITY SUPERPOWERS**

**Incident Response Firms:**
- Found Evil
- DOXED APTs
- Burned Infrastructure

**SOC Teams:**
- Went Hunting
- Prioritized Alerts
- Pursued Attribution
“Most companies are not using threat intelligence. Those that are, are not using internally sourced threat intelligence.”

- Rob Lee
“Most companies are not using threat intelligence. Those that are, are not using internally sourced threat intelligence.”

- Rob Lee
Threat Hunting + Threat Intel = ???

**FOCUS ON LOCAL THREAT INTELLIGENCE**

- AD Authentication Failures
- VPN logins
- IP Addresses from firewall scans
- Mail server logs
- Web proxy request logs
- Internal DNS logs
- Emails from the CFO!

Understanding Intelligence

**CONVERT THREAT DATA INTO THREAT INTELLIGENCE**

Data → Information → Tactical → Strategic

Find intersections with external threat intel

Focus On:
- Actors
- Infrastructure
- Domain Names
BEHOLD THE POWER OF ENRICHED PROXY LOGS

Event Decoration
Event Decoration

BEHOLD THE POWER OF ENRICHED PROXY LOGS

Find the Quick Wins

A DOMAIN CENTRIC APPROACH WILL UP-LEVEL YOUR TEAM

- Actors **borrow** IP addresses, but they **control** domains
- Domain names inherently **reveal intent**
- Whois records are **frequently identical** across registrations by the same actor
- Domain names need **supporting infrastructure**

Where are the domain names in your environment today?
Real World Example

Registrant Name: Reginald C. Rodman
Registrant Organization:
Registrant Street: 12 Heath Hill
Registrant City: Brookline
Registrant State/Province: Massachusetts
Registrant Postal Code: 02043
Registrant Country: United States
Registrant Phone: +1.5169081197
Registrant Email: procurement.alumatecsystem.com@gmail.com
Name Server: NS1.WORDPRESS.COM

googlledoc.com
Learning To Be Super

**Enrich** log data for context and targeting

**Pivot** through actor infrastructure

**Value** local threat intel data

**Focus** on domain names

---

There’s an app for that...

*SOLUTIONS FOR THREAT INTEL TEAMS & SOCS*

Iris Investigative Platform
Now with pDNS from Farsight (et al)

PhishEye Alerts

Enrichment & Investigation APIs
Splunk App Now, QRadar Soom
Threat Intel Platforms
Automation Platforms
`pip install domaintools_api`
THANK YOU!

MARK@DOMAINTOOLS.COM