INTELLIGENT-DATA

There are 2,645 network invasions every minute. It’s time to go on the offensive.

Yet, detection today is a post-event statement. Even Network Operation Center SIEM’s (Security Information and Event management) are post-event analysis that provide prevention for future attacks based on the past. **A paradigm shift in predictive detection is now possible with AI white hat botnets working for you.**

Continuous, automatic, autonomous detection – Available Now

Today’s attacks come from multiple ecosystems- 2nd & 3rd client partners (perhaps those even using your logo) SaaS applications, and Platforms (IaaS) used outside your own network.

Current solutions- There are 3 key current paths chosen:

I Conduct a **vulnerability scan** of the network – this discovers open avenues available for an attack via many factors, open ports, devices requiring patch management etc.

II Conduct a **PEN test**, (penetration test) - this requires a skilled hacker with some pre-knowledge of the network and then set him/her loose to break into the network.

III Hire a **Certified Ethical Hacker** (CEH) allow him/her to break into your network and report the findings. Generally limited time frame contracts.

Of course, many hire MSP’s or Managed Serviced SIEM’s to do *some* of this but they all ask for permissions which is not a benefit bad actor have and therefore tests start with bias.

ALL vulnerability testing and ALL PEN tests require that you provide information about your network, obtain permissions, or place assets (Virtual/On-Prem) – to conduct the test.

Challenge- How can your company truly go on the offensive in this 24x7x365 cyber-security war?
Is there a way to use AI tactics of a bad actor - but do no harm? How can one automate the actions of a CEH, actions that never sleep and set off NO false alarms?

A radical new approach to shadow risk detection.

- **CYCOGNITO** requires NO agents on the network. We will not ask for ANY *information about your network*. **Results are 100% unbiased.**
- **CYCOGNITO** uses automated A.I. Botnets from over 100 countries that never rest. **Your network is *continuously and autonomously subjected to simulated attacks that do NO harm and set off no false alarms.*** You will discover every vector outside your attack surface - identifying every known and unknow asset.
- **CYCOGNITO** provides a dashboard of all activities, assets, discoveries, and a prioritization list of all vectors based on the least resistant paths. Remediation steps with info links about the discovery help understand the threat.

What’s next- Intelligent-Data can tell you more about how **CYCOGNITO** can help you detect & predict your cyber-vulnerabilities. No information about your network is required (just like a bad actor has no pre-knowledge, nor any advantages) and the botnet will ‘boil the Internet ocean’ including all the ecosystems.

We will provide a no charge POV/POC for your review along with a **CYCOGNITO** data scientist team. **We get in** - you have no false alarms- and you learn at no charge how we did it. **Then you decide**.

bobr@intelligent-data.com **Boston Hqt.(Northeast) or** daniel@intelligent-data.com **Miami Hqt. / LATAM**