A CYCOGNITO SOLUTION BRIEF

Discover and Contextualize

Key Elements for Successful Exposure Management

Organizations today are exposed in more ways than they realize. Most organizations have 30% to 80% more externally facing IP addresses, servers or networks than are known by their IT or security teams. And it's not just assets, it's subsidiaries too – our recent "External Risk Insight Brief" found that Fortune 500 organizations were originally unaware of 10% to 30% of their own business units, brands or branches.[1]

1 *CyCognito's External Risk Insights Brief, https://www.cycognito.com/external-risk-insights*

The Problem

Discover, Inventory, and Map Your Exposed Risks

Understanding your external attack surface is the first step in uncovering unknown or unmanaged assets. But once you've discovered those assets, do you know where you're exposed? Which assets have vulnerabilities and lead to sensitive data or critical systems? Which organization owns the asset and can you map that ownership with evidence?

With CyCognito, find and understand your unknown assets, discover where you're exposed and map those risks to the entities that own them.

From Mapping to Enumeration; Discover What's Hidden

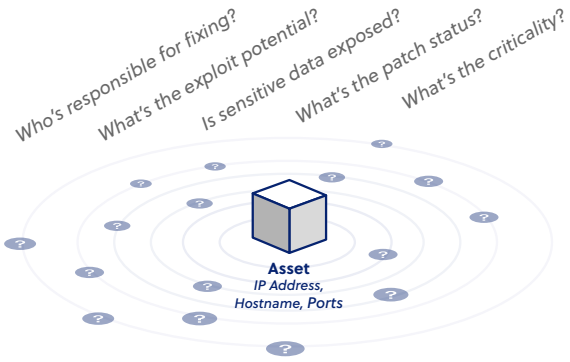
The CyCognito platform maps assets to the organization that owns them. To do this, CyCognito starts by finding all entities associated with the primary entity. The platform uses natural language processing (NLP) to consume and process terabytes of information across various open source intelligence (OSINT) such as financial reports, news articles, and sources like Crunchbase. Machine learning algorithms interpret the OSINT findings to map the organization and determine which subsidiary or business unit owns the asset. This results in a charted map of each asset and exposed risk tied to the organization that owns it, saving SecOps or other teams 4 to 10 hours per asset doing the same ownership attribution.[2]

Context, or the details about each asset, enables you to take action.

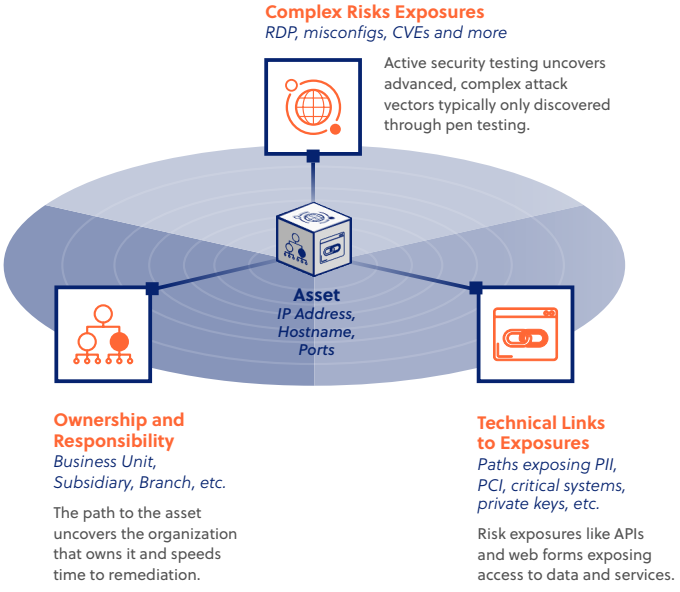
Find. Contextualize. Act.

Context, or the details about each asset, enables you to take action. It tells you technical details about the assets, what software versions are running, who the responsible organization is, if an exposure puts important data at risk and how discoverable and attractive it is to attackers. Having the right context connects you with insight to take action.

Lacking the correct data leaves you with questions.



CyCognito provides actionable context.



2 *CyCognito research communication with enterprise organizations.*

Context Fuels Cooperation Across Entities

Managing external risk exposure can be a challenging task for any large organization. Let's take a look at a real story about how a state government faced this challenge. A large state in the US recognized the need to get ahead of externally exposed risk across various entities that play an important role in serving its population. These included higher education institutions and utility companies that are outside of the state's direct control, yet if their data were breached it could have catastrophic consequences.

Despite not having direct control over these entities, the state still wanted to assess the potential risks across both public and private networks, to proactively notify them. This scenario while a state government, also applies commonly to commercial businesses that often have tens or even a hundred subsidiaries, brands, regional locations and more that connect to the parent organization.[3]

The incident proved the value of having the right context as evidence can be used to inform conversations across entities and help gain control of external risk exposure.

The CyCognito platform wasn't the first solution the state had considered to manage their external attack surface. The state was planning to purchase a competing solution from a vendor they've had a relationship with and were attempting to orchestrate a deal quickly. However, things changed when they found CyCognito, with a revolutionary approach to managing external risk exposures.

With the CyCognito platform, the state was able to alert a large city of a vulnerability with an Internet appliance used for content control and network security. The city was surprised as it was not even aware of the existence of the device in question. The IT Operations manager and user of the CyCognito platform said, "I was able to log in, tell him the IP address, and all of the details of how we found it." This changed the relationship with the city, and the now-customer proudly stated, "They were more than willing to work with us on future security endeavors."

The state then purchased the CyCognito platform over the competition and today uses its workflow automation APIs to integrate with the incumbent's ticketing systems.

"I was able to log in, tell him the IP address, and all of the details of how we found it." This changed the relationship with the city, and the now-customer proudly stated, "They were more than willing to work with us on future security endeavors."

—IT OPERATIONS AND USER OF CYCOGNITO

3 *According to CyCognito's External Risk Insights Brief, https://www.cycognito.com/external-risk-insights, we found that an average organization can have 104 subsidiaries and their security team is unaware of 10 to 31 of them. A subsidiary in this context can represent an entire business unit, brand or company.*

A CYCOGNITO SOLUTION BRIEF

Use Cases

Reconnaissance-Based Discovery.

Gaining an attacker's perspective with automated reconnaissance that maps your organization including business units, subsidiaries, branches, brands and more. Assets are then enumerated and tied to each entity. This uncovers paths of least resistance through unknown, yet connected entities that an attacker could exploit, but other solutions with seeded inputs would not find.

Natural language processing and machine learning process and correlate entities and their assets in a logical way.

Mapped ownership to business units or entities responsible.

When asking a business unit or subsidiary to take ownership of an exposed risk on an asset they own, proving they own it might be necessary. A discovery path for each asset helps aid conversation and illustrate how the asset they own puts your organization at risk.

Verifiable discovery paths through news publications, regulatory docs, industry databases and more.

Reduce the time validating the presence of an exposed issue.

With verifiable findings and continuous security testing, exposures are both uncovered and validated, including even OWASP Top 10 issues. The CyCognito approach is unlike other attack surface technologies that rely solely on basic port scanning that are fraught with false-positives or omit issues entirely.

Technical Value: network mapping, port scanning, OSINT, continuous application security testing and more.

Technical links that underscore importance.

A highly critical issue is prioritized based on what it connects to. For example, a vulnerable asset connected to a server is one thing. Knowing it's actually a database with potentially sensitive data vs. an empty server changes the importance significantly.

Links between machines including hyperlinks, gateways, usage of third-party code and resources.

We are CyCognito, a revolutionary approach to exposure and risk management driven to create positive business impact. We help organizations identify, understand and master their risk in profound new ways. **Rule Your Risk.**

For more information on CyCognito's External Attack Surface Management solution, go to **cycognito.com/how-it-works** or schedule a demo at **cycognito.com/demo-video**.

CYCOGNITO