CYCOGNITO

SOLUTION BRIEF

Scale Your Pen Test and Red Team Operations with CyCognito

Automated Reconnaissance and Active Testing across your full External Attack Surface

Black box penetration tests ("pen tests") are a staple of IT security teams. Tasked with identifying flaws and weaknesses across your digital infrastructure, pen testers and red teamers closely follow the approach of an unprivileged attacker, from reconnaissance, initial access, and even execution.

Unfortunately, the size of an organization's external attack surface coupled with pen test cost and delivery time forces many organizations to reduce test scope to known "crown jewel" assets – typically web applications and infrastructure – for quarterly or annual investigation. Even so, enterprise pen test costs are high, often over USD$100K annually and exceeding USD$1M for large organizations.[1]

Despite the rich insight they provide, today's rapidly changing risk landscape means a short shelf life for these point-in-time tests. Long gaps between tests and low coverage result in wasted opportunity and excessive risk.

Today's security teams can do more with pen testing resources

Reconnaissance is labor and time-intensive

Asset attribution, classification, and other context can take 5-10 hours per asset

Infrequent tests extend remediation times

Point-in-time tests on a subset of assets (often only 5-10%) lead to long remediation times, 12 months+

Manual data sharing is ineffective

Results shared manually through spreadsheets and email increase latency and reduce effectiveness

1. State of Pen Testing 2021 | Dark Reading Research survey of 108 cybersecurity and IT professionals involved in pen testing, January 2021

Designed by reconnaissance leaders from a globally recognized intelligence agency,

CyCognito built the discovery and active testing engines in its external attack surface management (EASM) platform to replicate an attacker's thought processes and reconnaissance workflows.

THE RESULT: a unique platform that automates the first phase of offensive cyber operation with deep, nation-state grade reconnaissance and active testing.

With CyCognito, organizations can effortlessly increase testing coverage from ~5% to ~100% and test cadence from quarterly/annually to weekly.

Scale your offensive security teams with CyCognito

Reconnaissance and attribution information when they need it

Replace time-consuming scanning/recon work with focused activities such as exploit chaining and lateral movement

Automated, continuous, active security testing delivers confidence

Over 25,000 high-quality security tests, across your full asset inventory

Reduce burnout and focus on meaningful issues

Automated workflows reduce manual tasks and allow teams to showcase personal value and efficiency

Case Study: Large Investment Company (F500, ~$300B Managed)

The Chief Information Security Officer of a large investment company had been striving to identify his organization's complete attack surface and most critical vulnerabilities, a challenge he'd been trying to solve in his role as a CISO for over five years.

"CyCognito delivers the attack techniques of a pen test," says the CISO. "We can use the CyCognito platform for an annual security assessment instead of a general penetration test and get a more effective result."

Help your pen test operations teams do more in less time

CyCognito automates many activities in the end-to-end pen testing process, enabling pen testing staff to focus on meaningful issues that require human decision.

The table below outlines what may be found in a US$50K-$100K standard pen test operation and how it compares to CyCognito's automated insight. A standard pen test scope is limited by time and asset numbers – CyCognito insight covers the full asset inventory.

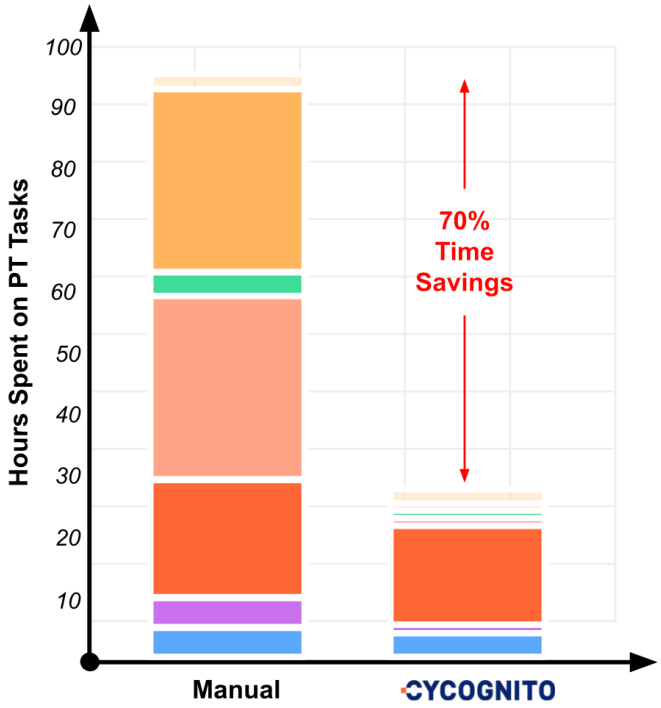
> Any enterprise that has to fulfill regulatory requirements or is required to do pen testing will see tremendous value after adopting the CyCognito platform"
>
> **Fortune 500/Global 2000 CISO**

Pen Test Phase	Activity	Standard PT	CyCognito
Scoping	Typical test scope	Partial (5-10%)	Full
	Uncover and map global organizational structure		✓
Reconnaissance/ Attribution/ Vulnerability Analysis	Uncover IP ranges	Manual	Automatic
	Build asset inventory	Partial	Global
	Investigate assets (OSINT, other tools)	✓	✓
	• Classify and fingerprint assets	✓	✓
	• Add business context to assets		✓
	• Add attribution context to assets		✓
	Identify CVEs through software versions	✓	✓
Prioritization	Based on severity (CVSS)	✓	✓
	Based on asset discoverability		✓
	Based on asset attractiveness		✓
	Based on threat intelligenc		✓
Testing	Active Tests/DAST	✓	✓
	High-risk exploitation activities	✓	
Reporting/ Recommendations	Evidence collection, findings, executive summary	✓	✓
	Remediation planning and prioritization		✓
	Frequency	Qtr/Annual	**Weekly**
	Complexity	Manual	**Automatic**
	Data Access	Manual	**UI, API**

Reduce a status quo pen test from weeks to days

It is not uncommon for a typical pen test to take two weeks. CyCognito's automated reconnaissance, prioritization, and low-risk active testing enable faster pivot to human-led active tests and a shorter completion time.

Typical PT Phase	Manual* 25% auto, 75% manual	Automated 99% automated
Scoping	1-2 hours	Same (Not Automated)
Reconnaissance / Attribution / Vulnerability Analysis	20-30 hours	~0 hours
Prioritization	1-3 hours	~0 hours
Testing - Low-risk DAST/Active Tests	20-30 hours	~0 hours
Testing - High-risk DAST/Active Tests	15-20 hours	Same (Not Automated)
Evidence collection, documentation	3-5 hours	~0 hours
Consuming information, building report	3-5 hours	Same (Not Automated)
Total	**63-95 hours**	**19-27 hours**



Find out more

CyCognito exceeds the external risk requirements of the largest and most complex organizations. Contact us to learn more about how CyCognito can increase the power of your pen testing program.

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO