A CYCOGNITO SOLUTION BRIEF

Prioritize Risk and Accelerate Remediation

Identifying infrastructure vulnerabilities and misconfigurations has always been a daunting challenge. Like most security teams, you're likely worried about your external-facing assets that could be present in public clouds, on remote-worker machines, or made public on subsidiary or partner networks. Vulnerabilities and misconfigurations are also a moving target, with new, more urgent issues appearing as your team attempts to schedule remediation of existing ones.

A CYCOGNITO SOLUTION BRIEF

The Problem

Teams often lack the time, resources, and budget to evaluate every issue holistically. Instead, they often rely on CVSS severity to prioritize issues, only focusing on "highs" and "criticals," or ranking by order of arrival. As a result, security teams are often left with an overwhelming list of poorly prioritized issues to fix, while lower severity exploits that affect critical infrastructure—like servers connected to PII or payment processors—are left unpatched.

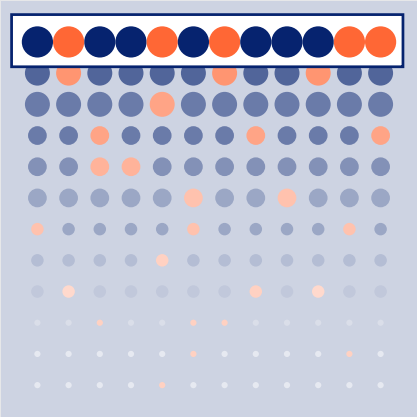
Intelligent, Automated Prioritization

CyCognito prioritization goes beyond CVSS scores by incorporating critical factors like asset classification, security testing results, curated threat intelligence, asset ownership, and attacker weaponization metrics to help your team direct your energy where it's needed most. Automatic asset attribution points your teams to the right technical owner, smoothing friction between teams and improving trust across them. With CyCognito's step-by-step guidance to resolve issues for every risk factor, you enable teams or owning entities to easily take action.

When your team makes progress, CyCognito makes it easy to automatically generate actionable remediation plans, view dashboards that validate external risks have been resolved, and create progress reports for executives and security leaders.

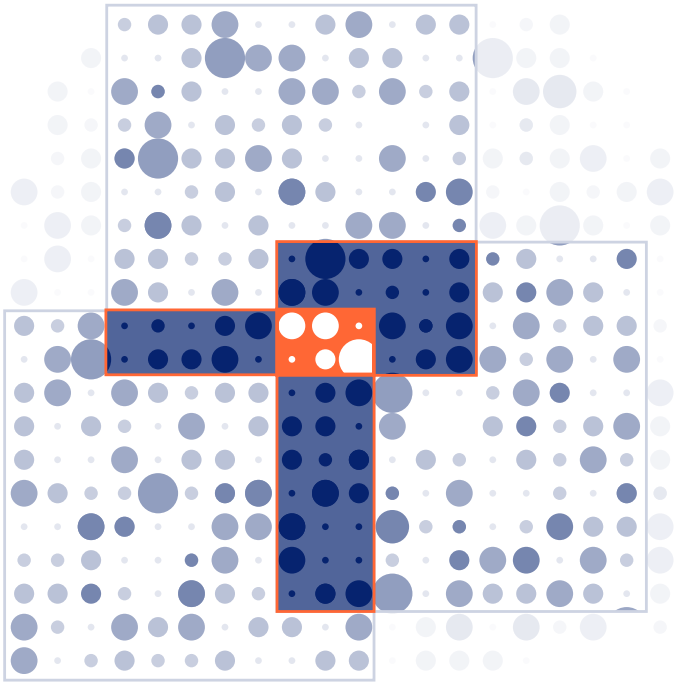
Prioritizing only by severity

misses lower severity issues that could be affecting critical assets and misses vital context.



CyCognito prioritization incorporates multi-dimensional factors

like asset attractiveness, availability of exploits, and attacker weaponization metrics to highlight the issues that pose the greatest risk to your organization.



Case Study

With new CVEs added to the database every 10 minutes on average[1], it's more important than ever for security teams to be able to focus on what really matters. Prioritizing these issues is both never-ending and can easily bog down a team forced to arbitrarily choose which issues to resolve and which to ignore. And the ones you ignore might be the most costly, exposing PII or payment systems. Fortunately, there's CyCognito.

A CISO for a multinational consumer goods conglomerate reported, "What I like about CyCognito is when I see a critical alert in there, I have confidence that it's correct, it's exploitable, it's been surveilled, and I know quickly if I want to validate that in the console itself."

CyCognito equips his team to jump directly into resolving the issue by providing in-platform evidence of how the issue was found and how to validate it. This CISO added, "the platform is telling me exactly what it used to find that alert, not some generic statement that it's vulnerable to a CVE, and then I gotta go research the CVE to figure out what's going on. The console has really helped my team jump... from identification to resolution using the information right in the tool."

When your security team is ready to take action on issues, CyCognito can help.

This same CISO stated, "CyCognito also helps you figure out, 'oh that's the Acme part of my organization. I know how to contact them, their IT operations team, and work with them on the remediation.' It's helping you both on the technical... side, but it's also helping you [understand] 'who do I go contact so I can start working on this remediation?'"

To jumpstart your team's remediation of issues, CyCognito has an extensive suite of integrations and workflows, including leading ticketing systems, SIEMs, and vulnerability management platforms.

Other products just give you an unranked list of problems. CyCognito gives you a prioritized list of issues to solve immediately and the tools to get started.

> **The platform is telling me exactly what it used to find that alert, not some generic statement that it's vulnerable."**
>
> —CISO FOR A MULTINATIONAL CONSUMER GOODS CONGLOMERATE

1 *Between January 1st and June 8th 2023, 12,460 CVEs were added to the NIST database, approximately 78 per day and 7 per hour. https://nvd/nist.gov*

A CYCOGNITO SOLUTION BRIEF

Use Cases

Planning Phased Remediation Plans with Goals

A strong remediation plan needs to define the issues or assets in scope for the effort, state the intended outcome, and provide reports on progress. CyCognito's in-platform Remediation Planner creates customized plans for organizations to raise their security grades, address troubled assets, and bring subsidiaries into compliance with the rest of the organization.

Built-in tools to visualize progress, identify next steps, and report up or down.

Workflow Automations Create Efficiency

Automation and integration with existing IT infrastructure can accelerate action, improve remediation times, and make communication between teams easier. If your IT team uses JIRA to create and manage tickets, the CyCognito platform's JIRA integration can automatically generate and task tickets to technical owners, complete with:

- Details about the issue
- How the asset was discovered and linked to the organization
- Step-by-step instructions to remediate the issue

Customizable workflows and integrations with Palo Alto Cortex XSOAR, single-sign-on, ServiceNow, JIRA, Slack, G Suite, Splunk, Zendesk, and Teams, with many more possible.

Respond to Advisories and News Items

When a new CISA advisory is released, it's all hands on deck to figure out which externally-exposed assets are affected and should be patched first. With CyCognito's Advisory Dashboard, security teams can view the CISA advisory, research additional context, and get a list of assets to remediate first.

Documented discovery path and automated identification and tasking of technical owners, for seamless action on advisories.

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