CYCOGNITO

DATA SHEET

Exploit Intelligence

Accelerate remediation efforts by focusing on exploitable vulnerabilities in your attack surface

BENEFITS

Focus on the most impactful issues on your attack surface - those being actively exploited by attackers in the wild.

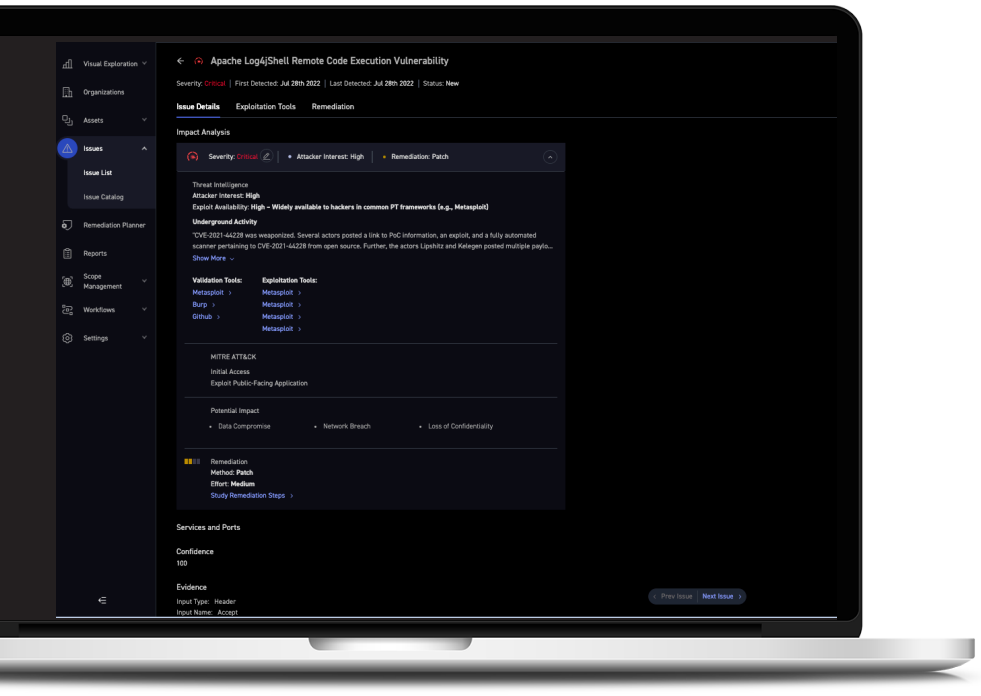
Easily and safely validate whether an issue in your attack surface is exploitable.

Understand what an attacker would do to exploit a weakness or vulnerability and the possible traces (IOCs) of an attack.

Safely simulate an attack while testing your defenses

CyCognito Exploit Intelligence offers an end-to-end solution that prioritizes which risks to remediate immediately—before they are exploited—by proactively discovering external assets, testing vulnerabilities, and providing expert threat- and risk-based insight.

Developed to help security teams focus on the most critical risks first, Exploit Intelligence creates in-platform advisories about threats being exploited in-the-wild and aligns them with assets in the organization's external attack surface. Operations teams can spend their time fixing issues instead of figuring out how to fix issues with our prescriptive and intelligent remediation guidance, supporting evidence and the ability to simulate the remediation in a virtual environment lab.



Exploit Intelligence in Action

The CyCognito platform's Exploit Intelligence capability gives teams all they need to swiftly respond to emerging threats in days, rather than weeks.

01. Time is of the essence

Adversaries consistently scan target networks for critical and high vulnerabilities within days of the vulnerability's public disclosure (source:joint advisory by NSA,CISA,FBI)

02. Be efficient

Leverage curated threat intelligence to show how vulnerabilities are being actively exploited by attackers in the wild and how those threats map to vulnerabilities in your attack surface.

03. Quickly Assess Impact

A detailed summary graph paints a clear picture of assets at risk and shows what subset of assets remain vulnerable and what subset are protected.

04. Know who to approach to remedy

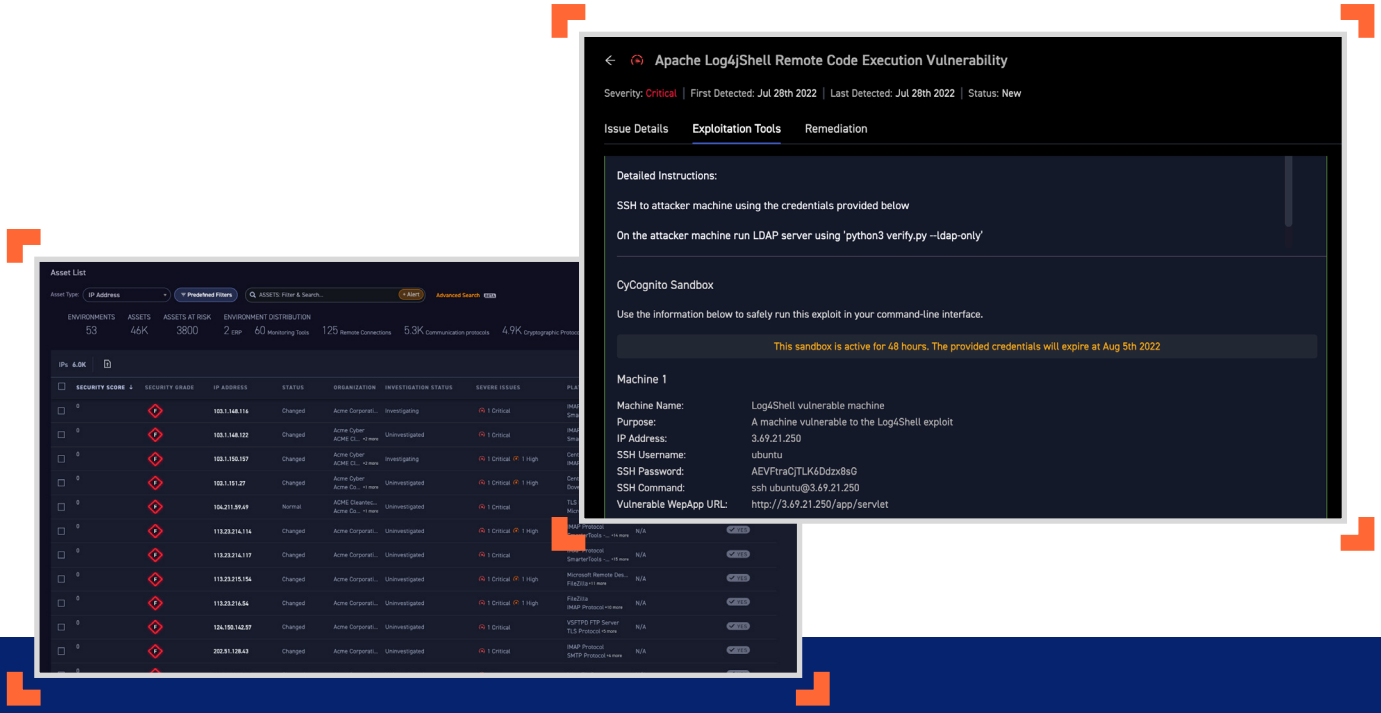
Receive evidence that identifies the organization responsible for remediating the vulnerability assets

05. Verify and Act With Confidence

Safely simulate the remediation with guidance in your CyCognito virtual lab before alerting the right Security Operations, Risk and IT teams.

06. Remediate and Repeat

Integrations provide remediation guidance and validation steps with SIEM/SOAR and ticketing tools, allowing for quicker MTTR. Once the issue has been remediated, CyCognito will validate that the vulnerability has been resolved.



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