EXPLOIT INTELLIGENCE

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

CyCognito Exploit Intelligence provides your security operations, penetration testing, and red teams with threat intelligence tailored to your attack surface and its vulnerabilities. In addition to threat advisories, your teams get step-by-step guidance on how to safely simulate attacks that validate your countermeasures. This enables your organization to expedite validation and remediation of the most critical risks in your external attack surface.

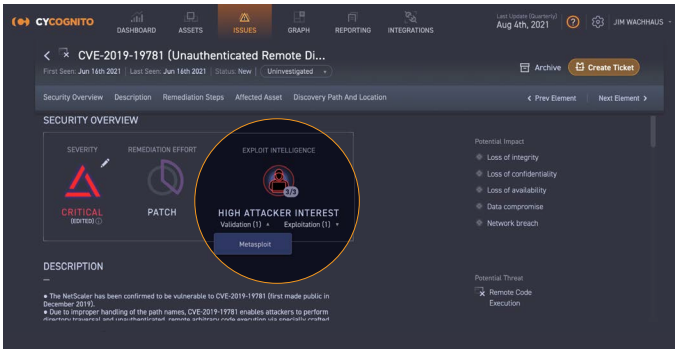
Vulnerability management is one of the most important and most difficult areas of security today. With thousands of vulnerabilities new and old to monitor and remediate, it's incredibly hard for teams to prioritize (and then fix) those which present the most risk. Often, this prioritization is done simply using CVSS scores. And sometimes it's informed by red teams when they find and exploit a vulnerability in their attack surface.

Taking the perspective of an attacker performing reconnaissance, CyCognito actively discovers your entire external attack surface and then tests your external assets for security gaps and vulnerabilities. Once detected, the platform provides guidance and prioritization to intelligently fix issues in the most efficient and effective way.

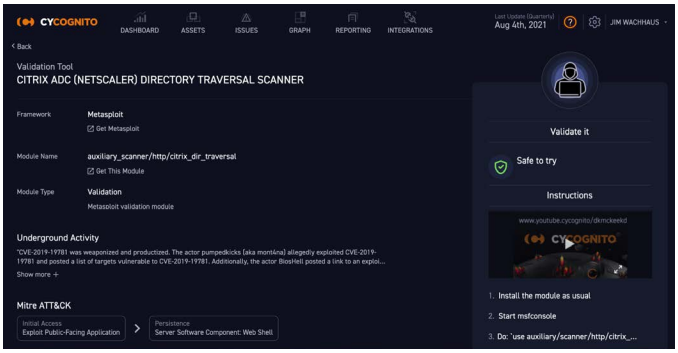
BENEFITS

- Focus on the most impactful issues on your attack surface — those being actively exploited by attackers in the wild
- Easily validate whether an issue in your attack surface is exploitable
- Understand what an attacker would do to exploit a weakness or vulnerability
- Safely simulate an attack while testing your defenses by following step-by-step instructions

Enable use cases like:



Identifying a security issue affecting a Citrix NetScaler asset where an exploit is available in-the-wild.



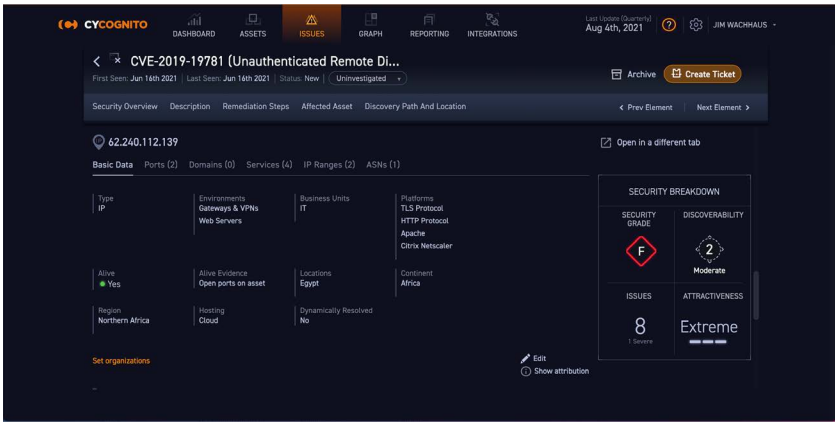
Simulate and validate exploits using step-by-step instructions that safely exploit vulnerabilities and simulate breaches to validate risk.

The CyCognito platform's Exploit Intelligence capability gives teams all they need to perform comprehensive security testing and attack exercises.

01

Begin With Vulnerability Intelligence

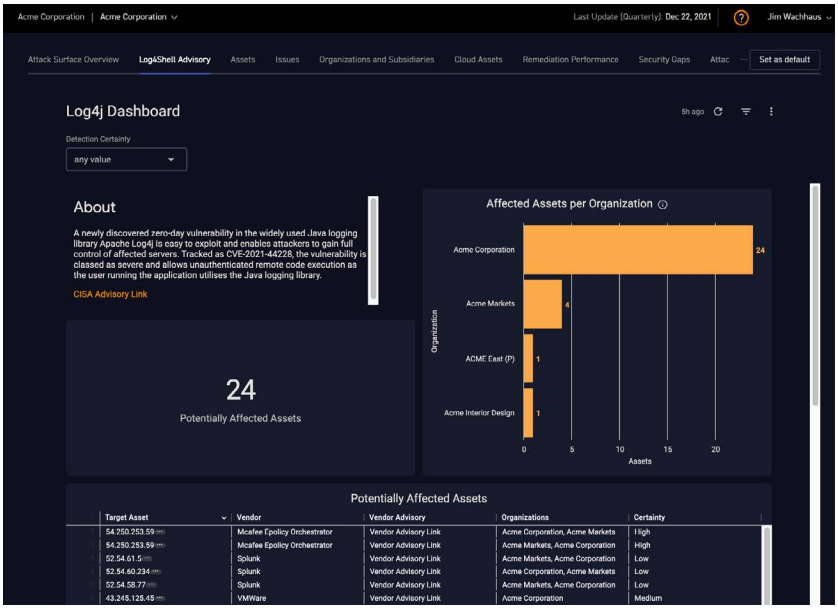
Identify vulnerabilities in asset configuration or software without configuring a scan.



02

Incorporate Threat Intelligence

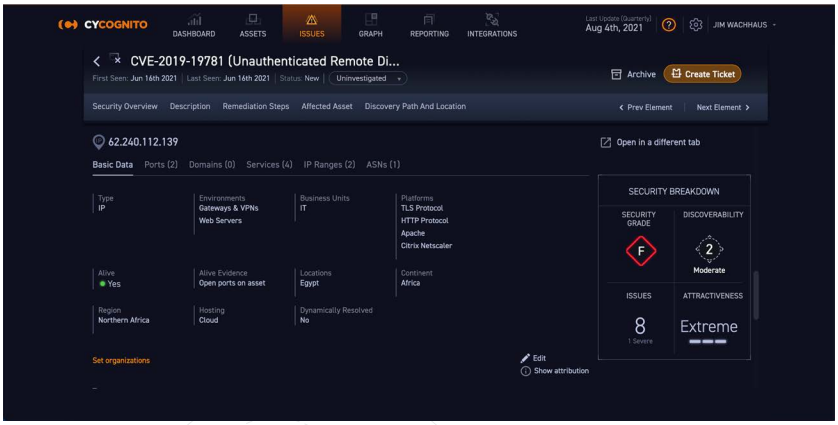
Understand how vulnerabilities are being actively exploited by attackers and how those threats map to vulnerabilities in your attack surface.



03

Simulate and Validate Exploits

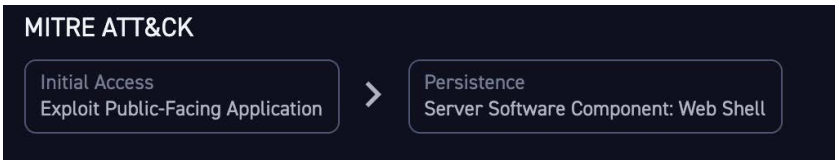
Use step-by-step instructions to safely exploit vulnerabilities and simulate breaches to democratize red teaming. Look for Indicators Of Compromises in your SIEM, XDR and other security countermeasures.



04

Communicate to Stakeholders

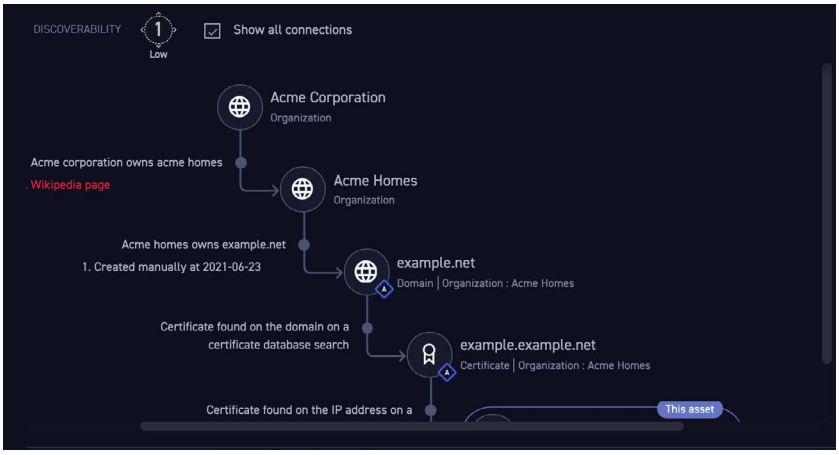
Leverage MITRE ATT&CK Framework mapping to better communicate and understand adversary behaviors.



05

See Asset Discoverability

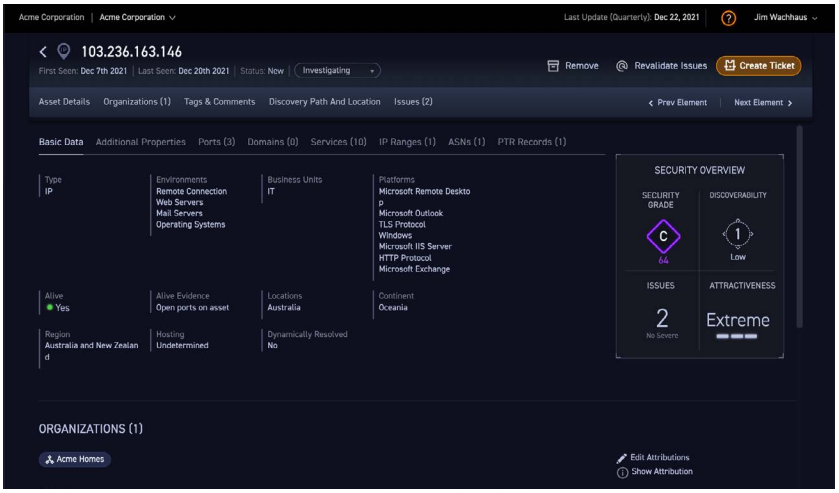
See how the asset was discovered using the platform's Discovery Path view so you can defend it appropriately.



06

Understand Asset Business Context

Get asset intelligence, including what the asset does, who owns it, and where it's located. Context that speeds remediation.



WATCH DEMO

SCHEDULE A PERSONALIZED DEMO

CYCOGNITO

420 Florence Street
Palo Alto, CA 94301
cycognito.com

CyCognito is solving one of the most fundamental business problems in cybersecurity: the need to understand how attackers view your organization, where they are most likely to break in, and how you can eliminate that risk.