SOLUTION BRIEF: CYCOGNITO + AXONIUS JSB

Identify and Secure Exposed Assets — Securing Your Attack Surface Inside and Out

CyCognito and Axonius help Security and IT Operations teams identify, protect, and manage their cyber asset attack surface.

The Challenge

The cyber attack surface is growing at an unprecedented rate. The rapid adoption of cloud services, rise of remote access, use of ephemeral DevOps environments, and thousands of unmanaged devices accessing corporate and corporate-adjacent networks has created constant change. The resulting task of identifying and managing an organization's attack surface has become complex and time consuming.

Exposure management is top of mind, and organizations need the right tools to identify what assets exist, locate and prioritize vulnerabilities on those assets, and efficiently take action to remediate gaps in security policy. Traditional security tools help but often are limited to known issues on known assets, work in silos and are unable to provide a holistic view of an organization's risk posture. Additionally, a legacy focus on internal threat actors leave externally-exposed assets, systems and networks ripe for exploitation.

The lack of visibility, combined with an ever expanding cyber attack surface, leave many organizations struggling to meet corporate requirements for risk and vulnerability management. It thus falls upon Security and Operations teams to understand the depth and breadth of their attack surface, as well as build a plan of action to reduce exposure.

The Solution

The first step in addressing the above challenges is gaining complete visibility into the cyber asset attack surface. This includes external and internal assets, asset-related context, and risk.

The Axonius Platform connects via simple application programming interface (API) connections to existing toolsets and collects context enriched data about each internal asset. With the CyCognito adapter connected, organizations are delivered a comprehensive analysis of their external exposures and risk providing a unified, holistic view of the attack surface.

Axonius and CyCognito together provide a broad picture of risk allowing mutual customers to efficiently prioritize threats based on their potential for real-world risk and damage. Attack vectors, unmanaged devices and users, users with privileged access and more are surfaced and presented uniformly to deliver Security and IT teams the visibility they need to efficiently and effectively prioritize and remediate issues.

How It Works

1

Connect the CyCognito Adapter

Once CyCognito credentials are supplied, the Axonius Adapter fetches asset and vulnerability data from CyCognito and populates Axonius via a simple API key.

2

Identify Security Coverage Gaps

The Axonius Query Wizard will help organizations quickly and easily surface new assets, vulnerable software, open ports, missing patches, and more. Additionally, Axonius provides consistent verification that all appropriate assets have been examined by Cyconito making the integration more effective in the environment.

3

Automate Enforcement

Take Automated action against prioritized threats via the Axonius Enforcement Center or via the CyCognito Community Library.

Key Benefits

Continuous and Complete Discovery

CyCognito continuously discovers your entire external attack surface while Axonius, via 800+ connected data sources from commonly used security tools, collects asset-related data from the internal attack surface. Together, we provide continuous, comprehensive cyber asset discovery allowing organizations to easily find and eliminate complete blind spots such as rogue networks and exposed cloud instances.

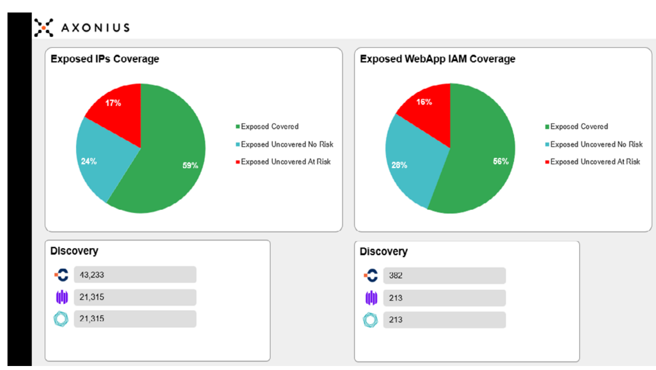

Figure 1. Visibility into assets at the greatest risk from an attacker's perspective

Prioritized Vulnerability Remediation

Prioritized remediation guidance based on asset criticality, business impact, vulnerability severity, external exposure and potential risk for exploitation.

Accelerate Remediation

Operationalize remediation tasks across your entire enterprise in the Axonius Enforcement Center using our holistic view of security to close the window of vulnerability more rapidly and reduce the risk of breach.

Eliminate Manual Processes

Automate asset discovery, remediation prioritization, and security policy enforcement.

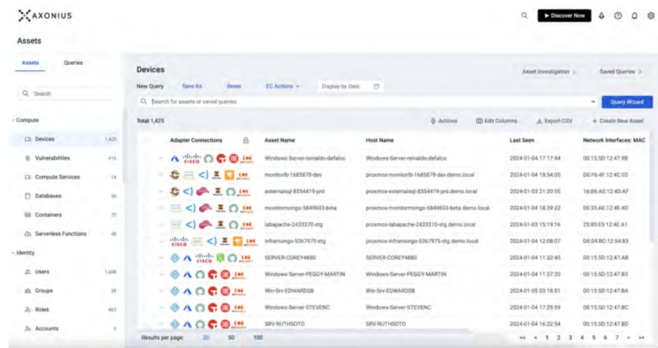

Figure 2. Seamless integration of CyCognito into the Axonius platform

About CyCognito

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. It does this with a category-defining, transformative platform that automates offensive cybersecurity operations to provide reconnaissance capabilities superior to those of attackers.

About Axonius

Axonius gives customers the confidence to control complexity by mitigating threats, navigation risk, automating response actions, and informing business level strategy. By seamlessly integrating with over 800 security and IT data sources, the Axonius platform delivers a true system of record for digital infrastructure, including hardware, software, SaaS apps, cloud, user identities, and more.

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-Axonius-SB-Jan2024