AXONIUS

CASE STUDY

A GLOBAL SPECIALTY RETAILER ACCELERATES TIME TO VALUE WITH AXONIUS

A LEADING GLOBAL RETAILER THAT SPECIALIZES IN APPAREL AND ACCESSORIES FOR MEN, WOMEN, AND CHILDREN THROUGH NUMEROUS BRANDS.

KEY CHALLENGES

- Inability to understand its asset footprint
- Lost person-hours to assess and mitigate zero-day vulnerabilities
- Limited ability to track employee equipment, like laptops

SOLUTION

Axonius Cybersecurity Asset Management Platform

RESULTS

The global specialty retailer implemented Axonius for a comprehensive, accurate, and reliable asset inventory, providing greater insight into its asset footprint and valuable ROI in time and resources.

> **"It takes minutes (not days) by one person (not the whole team) to get the information we need. Interestingly enough, Axonius also helps us quickly get to the bottom of almost every other asset-related question that we can dream up."**
>
> *– Staff senior security engineer*

KNOW THYSELF, KNOW THY ASSETS

For a global specialty retailer, obtaining an accurate and reliable asset inventory was one of its biggest challenges. And for the retailer's staff senior security engineer, who works with the data engineering, infrastructure, and architecture teams, having an up-to-date asset inventory was key to better understand the digital environment of these teams.

"I have shaped my life and personal philosophy on the basis of the Delphic Maxim, 'know thyself'," they said. "It can be a struggle to come to terms

with what you have. There can be a lot to uncover and unpack. And there's bound to be a ghost at the back of your closet — no matter where you live."

"Gathering an inventory of what you have — the good, the bad, and the egregious — is the first step forward into a better future," they continued. "It's no wonder that it's at the very top of the SANS 20 CSC list — it's paramount to establish a baseline of what you've got. Only then can you figure out what to do about it or in other words, 'know thy assets'."

Without a clear understanding of what was happening, the security team struggled to answer asset inventory-related questions accurately and quickly. This issue was compounded when major vulnerabilities or cyberthreats occurred.

"You have to drop everything to figure out the organizational impact of the newest zero day that's in the news," the staff senior security engineer explained. "That's an all-hands struggle that would completely derail an already packed schedule of high-priority meetings. And any stuff we didn't get done that week, we'd have to shoehorn it into the next week."

Assessing and reacting to security threats or incidents was requiring too much time and resources. For the retailer's security team, it was time to reevaluate how their asset inventorying was done.

MAXIMIZING TIME AND RESOURCES WITH AXONIUS

Initially, the security team received funding for a project with the goal of getting, correlating, and deduping asset data from multiple disparate systems and integrating it into ServiceNow.

As a key component of the solution, the retailer's security team was going to work with a contractor to write a proprietary set of code and an associated database. But that all changed when the retailer's CISO attended a conference and heard about Axonius.

During the proof of concept (PoC) stage, the retailer's security team realized Axonius could do more than fulfill their project's goal. In fact, the Axonius cybersecurity asset management solution could resolve a number of "ongoing asset-centric and efficiency issues."

"We saw so much potential," the staff senior security engineer said. "Axonius came up with tons of really interesting use cases, like looking at the data of what we have and then finding some shady backdoor software on 25 computers. We didn't know that Axonius could do that going in. [It] opened our eyes to problems we didn't even know we had — and taught us how to solve them."

"We could do it with an automated system and that's really what was great," they added.

Now when the retailer's CISO approaches the security team about the latest emergency, they can "calmly" log into the Axonius console and have a comprehensive, accurate, and reliable understanding of their asset footprint and the impact to their organization.

"After spinning up Axonius and configuring data ingestion from 25 different systems, with some fine-tuning and a splash of moxie, we can now leave the correlation and deduplication to the Axonius algorithms," the staff senior security engineer noted.

"It takes minutes (not days) by one person (not the whole team) to get the information we need," they continued. "Interestingly enough, Axonius also helps us quickly get to the bottom of almost every other asset-related question that we can dream up."

The security team started to field data requests from other teams. Almost always, Axonius had the answer to these requests. Now the retailer's security team has started down the path of integrating other teams into and training them on the Axonius platform.

DISCOVERING REAL VALUE IN A CYBERSECURITY ASSET INVENTORY

Not only does the security team have a better understanding of the asset footprint, they're also experiencing valuable ROI in time and resources.

Prior to leveraging Axonius, the staff senior security engineer estimated it took up to 50 hours of people's time to tackle a major zero-day vulnerability every month. That meant either the staff senior security engineer spent almost all of their time mitigating the problem, other team members helped out, or other teams got involved. All told, they believed major zero-day incidents cost the retailer about $60,000 a month in lost time and resources.

Axonius also helps the security team track the retailer's equipment. In the wake of the pandemic, the organization's employees continue to work remotely. Before implementing Axonius, the security team struggled to track whether employees returned their laptops or other equipment.

The staff senior security engineer estimates unreturned equipment totaled about 5% in costs every month. Now with Axonius, the retailer can recover about $10,000 a month in equipment — a total of $120,000 a year.

"With the two major things I mentioned here alone, that's maybe $180,000 a year in savings already — and that's significant," they said.

When it comes to working with Axonius, the staff senior security engineer found the customer service team "has been top notch from day one."

"It's the speed from when I bring up the problem to the time that it gets fixed — it's a matter of an hour or a couple of days, but definitely within a week or two," they said. "And that includes building new adapters or troubleshooting and fixing issues that we find with existing adapters. They're extremely responsive and that's a beautiful thing."

Axonius gives customers the confidence to control complexity by mitigating threats, navigating risk, automating response actions, and informing business-level strategy. With solutions for both cyber asset attack surface management (CAASM) and SaaS management, Axonius is deployed in minutes and integrates with hundreds of data sources to provide a comprehensive asset inventory, uncover gaps, and automatically validate and enforce policies.

Interested in what Axonius can do for you?

LET'S TALK