AXONIUS

CUSTOMER CASE STUDY

Lionbridge Powers a Strong Security Program With Axonius

LIONBRIDGE

Lionbridge helps companies connect with their global customers and employees by delivering translation, content creation, and localization solutions in 350+ languages. Lionbridge maintains solution centers in 26 countries.

EMPLOYEES

6,000+

KEY CHALLENGES

Getting accurate and quick answers to asset-related questions, maintaining an up-to-date asset inventory, and ensuring security control coverage.

SOLUTION

Axonius Cybersecurity Asset Management Platform

RESULTS

Lionbridge gained a single source of truth into their asset inventory and configuration, automated security control validation, accelerated incident response investigation, and strengthened their security program using Axonius.

Seeking Asset Visibility

Quickly understanding the environment they're tasked with protecting is top of mind for most security leaders when transitioning to a new job. For Doug Graham, chief trust officer at Lionbridge, the priority was no different.

In 2019, Graham took on the responsibility of building a robust security program across Lionbridge. The first step in the process was understanding the assets he was trying to protect, and the coverage and effectiveness of the security controls in place.

"Simply put, if you don't know about an asset, you can't protect it," Graham said.

But maintaining a current and accurate asset inventory – and getting quick answers to asset-related questions – was turning out to be an "uphill struggle." Factors like demands for faster provisioning and a rapid move to the cloud were driving further complexity.

"As I looked at the assets we had across the organization, the data was all there in various different systems. If I asked the right person in IT, I could get the right piece of information – but it was a complex process," Graham said.

Without a centralized tool that could correlate data across all these different sources, the team had to "rely heavily on this institutional knowledge," he said.

Taking Action With Axonius

Graham quickly realized that his team needed:

- A simpler, faster, and more effective way of getting enough context to secure assets
- An automated process for accessing asset information

Graham was familiar with the Axonius founders and the technology from a previous company he'd worked at. He quickly brought in the Axonius team to put together a proof of value to see how the platform would address his security team's challenges.

Today, Axonius enables Lionbridge to correlate data from 25 different data sources across their on-prem and cloud infrastructure and applications, building a single source of truth for inventory and configuration.

The platform allows the team to get an accurate, up-to-date, machine-level inventory (everything from network devices, servers, workstations, cloud instances, and more) and provides a user-level inventory (different types and classes of users).

> “We rely on Axonius to give us that solid foundation that we can build our more advanced controls on top of.

DOUG GRAHAM
CHIEF TRUST OFFICER, LIONBRIDGE

“This allows us to create a set of complex queries, and lets us see things like the coverage of our security controls and how effective they are,” Graham said.

Graham noted that the Axonius team has been “wonderful” throughout the entire process. From helping with deployment, to building queries, navigating the information, understanding the connectors, and where the correlation points are, the Axonius team is very responsive and supportive, he added.

“We rely on Axonius to give us that solid foundation that we can build our more advanced controls on top of,” he said.

A Powerful Incident Response Tool

Apart from providing context about software and hardware assets, the tool also provides a consolidated inventory for user information. Adding the user context to assets also allows for “marrying the traditional system inventory with a user inventory,” showcasing the interaction of both together, Graham said.

This helps security analysts answer critical incident response questions, like:

- Which devices and users were associated with the alerts?
- Where are the devices located?
- What software is running on the device?
- Which users are associated with the device?

“When you start pulling together a lot of that information into a single pane of glass and put that in front of an incident responder, then it makes their time to triage a lot quicker,” Graham said. “Because the information is there, and they don’t have to go across multiple areas to get that.”

> “I’m not sure that we could have done what we are doing today without Axonius.

DOUG GRAHAM
CHIEF TRUST OFFICER, LIONBRIDGE

Transcending Beyond a Security Tool

While Axonius was brought in as a security tool, it’s now “50% an operational tool and 50% a security tool,” Graham said.

The biggest testament to the results has been the adoption of this tool by the IT and engineering (including DevOps) teams. These teams are building their own use cases, charts, and metrics, he said.

Axonius also doubles as a governance tool, he said, because the security team can go in and look at these IT dashboards and make sure IT teams have the tools available to do their work effectively.

“Axonius provides us with a single source of visibility and a single source of truth. We’re no longer arguing about what’s there and what’s not there, what’s been patched and what’s not been patched, and what coverage looks like. Without a tool like Axonius, we would spend more time arguing about the data than looking into the underlying problem,” he said.

Staying Ahead of Cyber Attackers

Staying ahead of threat actors requires security and IT teams to have an accurate view of what’s within their environment, Graham said.

That’s because, sophisticated cyber attackers spend a long time learning about a company’s network and what its inventory looks like, during the reconnaissance phase. And if they know them better than the company does, that becomes a problem, he said.

“So, my recommendation would be: if you don’t have that view [of your assets], you’ve got to get it,” he said. “Axonius is a way that you’re going to be able to pull that together and get it very quickly. Then you can start taking action on the inevitable gaps that you’re going to discover in your coverage. It will make your security program stronger.”