AXONIUS

CASE STUDY

CITY OF LOS ANGELES ENHANCES VISIBILITY INTO ENTIRE ATTACK SURFACE THROUGH AXONIUS

AS THE SECOND-MOST POPULOUS CITY IN THE U.S., THE CITY OF LOS ANGELES IS A MEGACITY. IT'S HOME TO ABOUT 4 MILLION RESIDENTS AND 250,000 BUSINESSES. ON AVERAGE, LOS ANGELES HOSTS ABOUT 50 MILLION VISITORS EVERY YEAR.

EMPLOYEES

50,000 full-time employees

KEY CHALLENGES

- Limited insight into assets across all departments
- Different (and vast) department integrations
- Lack of visibility into internal attack surface

SOLUTION

Axonius Cybersecurity
Asset Management Platform

RESULTS

The City of Los Angeles leveraged Axonius for a comprehensive, always up-to-date asset inventory — helping them gain greater insight into their endpoints, enhance visibility into their entire attack surface, reemphasize policies and procedures, and support forward-thinking decision-making and initiatives.

> **When you're talking about attack surface management, the key element is good asset management. You've got to have a good inventory of what you have. You've got to know what you are protecting.**
>
> *- Tim Lee, CISO, City of Los Angeles*

KNOW YOURSELF, KNOW YOUR ENEMY

Protecting, mitigating, and responding to cyberattacks is never easy. The process is — by nature — complex.

Now imagine doing so for the second-largest city in the United States: Los Angeles. With 42 departments like the Port of Los Angeles and Department of Water and Power (and their critical infrastructure), ensuring situational awareness is at the forefront of the city's cybersecurity efforts.

“Our cybersecurity strategy is based on a very simple, straightforward concept: know yourself and know your enemy,” said Tim Lee, CISO for the City of Los Angeles. “We’ve got to have a clear picture of what we are protecting, and what are the assets in our protection domain.”

Los Angeles has centralized its cybersecurity efforts through the Cyber Intrusion Command Center, the city’s cybersecurity working group that leads cybersecurity preparation and response to critical security incidents. The working group includes the city’s department IT managers and CISOs, along with federal and state law enforcement partners.

As part of the city’s cybersecurity efforts, the Integrated Security Operations Center (ISOC) identifies, mitigates, and coordinates responses not only for themselves, but for their partners. The ISOC works as an integration point for the security teams and security operations centers of city departments, including the Los Angeles World Airport, the Los Angeles Police Department (the third-largest municipal police department in the U.S.), the Department of Water and Power, and the Port of Los Angeles. The center also provides technical expertise and support to all city departments on improving departmental security posture.

“We're such a large organization and we have so many different department integrations that are really important for us,” explained Daniel Clark Lee, manager of ISOC. “And one of our biggest pain points is having a lot of people using a lot of different tools or a lot of different things in there.”

This all made for an enormous — and complex — attack surface to protect. For the city’s cybersecurity team, assuring the internal side of the attack surface is as secure as the external (or public facing) side is a top concern.

“One of the other issues we had with internal attack surface management is it's fairly scoped down to things like Active Directory, or looks at only certain assets that might be missing patches, CVEs, or vulnerabilities,” said Daniel Clark Lee.

Along with the lack of visibility, the amount of disparate tools, and the concern to protect the entire attack surface, another need cropped up. Tim Lee and the ISOC team found they needed a solution that would help with cybersecurity’s efforts more effectively and efficiently. That need became a catalyst to search for a cybersecurity asset management solution.

“When you’re talking about attack surface management, the key element is good asset management,” Tim Lee said. “You’ve got to have a good inventory of what you have. You’ve got to know what you are protecting.”

A VIEW THROUGH A "SINGLE PANE OF GLASS"

The city's security team heard about the Axonius Cybersecurity Asset Management platform while they were researching cybersecurity asset management solutions. Axonius was one of three companies selected to the proof of concept (POC) stage.

Cesar Alvarado, senior SOC analyst for ISOC, oversaw the POC process. One of the top priorities during this stage was using the solutions to discover endpoint detection and response (EDR) installations.

"Axonius has helped us identify unmanaged devices without proper EDR installation and patch management levels," Alvarado said. "They provided excellent customer support throughout our deployment process. For example, Axonius already had an adapter for a vendor that we were using; however, the adapter was not providing information that we needed. Axonius quickly worked on improving their adapter to provide the information that we were missing."

With Axonius, the data collection and aggregation process is more efficient. Flexibility and visibility into data collection is vital, especially now. In early 2023, the City of Los Angeles reported a 20-times increase in attempts to compromise the city's systems and networks.[1]

"We need to be flexible and expandable, so either it could be 2,000 assets or 20,000," Tim Lee said. "It should be able to easily expand when we need it to. And Axonius gives us a lot of advantages in that area."

Asset data collection is key for the ISOC. The ISOC collects and correlates logs and events for the city's departments.

"Being able to integrate a lot of different tools and aggregate all that data into one kind of single pane of glass has been really important for us," Daniel Clark Lee added.

MEASURING THE PROTECTION DOMAIN WITH AXONIUS

Along with more situational awareness and easier data collection, the ISOC team has greater visibility into vulnerabilities. Specifically, they're identifying vulnerabilities through the Axonius platform more efficiently.

[1] "ITA Spotlight of the Month, Spring 2023", Information Technology Agency, City of Los Angeles, April 28, 2023.

According to Daniel Clark Lee, his team would switch between four or five different tools to find out which devices had alerts or compromises. It took time and resources away from day-to-day tasks. The ISOC team can now quickly identify compromised devices and find the users that are associated with specific devices.

The Axonius platform has quickly become one of Alvarado's go-to tools for alert investigations. Alvarado recently used Axonius to look into the alerts around IP phones. He had visibility into whether anyone in any of the city's departments were using the models in question.

"We didn't have any of them on that occasion, but it's good to have the peace of mind so we can answer questions like that," Alvardo said.

The ISOC is also receiving insight into any non-compliant access to the network, enacting layer policy enforcement when the time comes. If an issue appears, the ISOC team can take different measures, like reminding a department to follow the city's cybersecurity standards.

Axonius has helped Tim Lee with measuring and quantifying the City of Los Angeles' protection domain — and the ISOC's scope of responsibility.

"Now we can get into the endpoint level," Tim Lee said. "For example, under our protection umbrella, we have 87,000 assets that are connected to our network. It's easier for me to present or share this information with the business executives."

"We can quantify the scope and then the potential impact," he continued. "Not only is the information measurable, it's actionable, too. Axonius enhances our capabilities on threat hunting, investigations, and situational awareness."

For Tim Lee, the Axonius platform has helped him with decision-making and forward-looking initiatives, like Zero Trust.

"When you have a clear picture on the scope and domain of what you're protecting, then your strategy and your program is very targeted and very accurate," he said. "Otherwise, you're in this blind mode. Your cybersecurity program is not effective and your budget is not defensible. And then you are wasting resources, too."

"When you have good cybersecurity situational awareness, you can make an informed decision and make your cyber defense strategy more effective and efficient, " Tim Lee continued. "The information that we get from Axonius is one of the elements that support this process."

EXPERIENCE THE DIFFERENCE

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

AXONIUS