CASE STUDY

SWIFTLY SECURING A LARGE PUBLIC VENUE POST-BREACH

Cincinnati Museum Center

THE CUSTOMER
Cincinnati Museum Center

INDUSTRY
Large Public Venue

THE SOLUTIONS
Migration from compromised network environments to secure ones, 24x7 day-one support, tighter security solutions

BENEFITS

- The ability to return to servicing guests swiftly
- More robust security posture
- Better-protected networks and devices
- Regular architecture reviews
- Up-to-date patching

THE SITUATION

The Cincinnati Museum Center opened its doors in 1990 and has been cultivating an environment of learning and discovery ever since. With thousands of displays and events covering history, natural science, and fine art, the Museum Center has proven to be an invaluable educational and cultural resource to the people of Indiana, Kentucky, and Ohio – as well as across the nation.

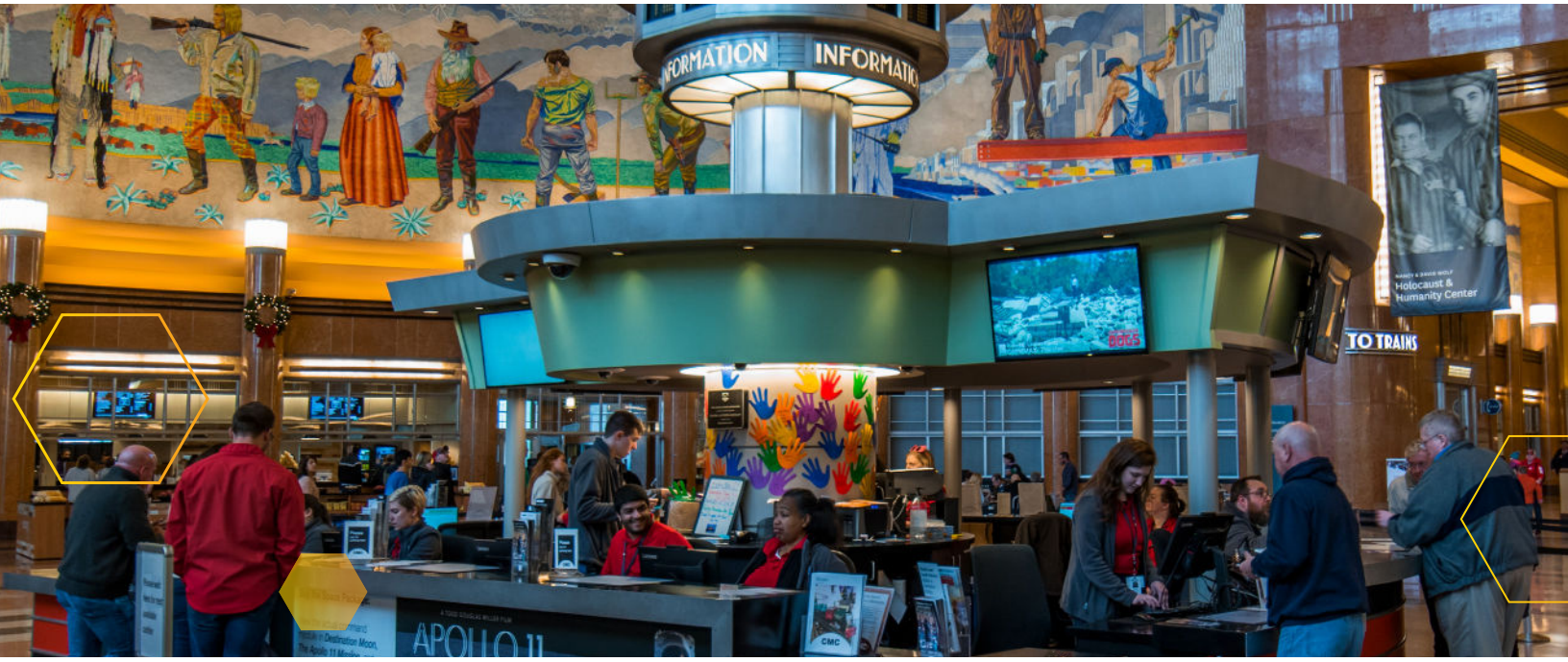
Undeniably, the role the Cincinnati Museum Center (CMC) fills within its community is invaluable. That's why when CMC was hit by a systemwide security incident in early 2022, it was a race against the clock to get them back on their feet. "People don't realize the extent to which these things happen," remarked David Zlatic, Chief Technology Officer for Cincinnati Museum Center. "They only think [security incidents are] happening at these larger organizations, like CNN…but they happen every day, all over the world."

The incident came "out of the blue" on a Saturday night, when CMC had a threat actor within their IT environment. Threat actors tend to target systems when they believe people will be away and monitoring will be at a minimum. David Zlatic and CMC's savvy IT team was able to figure out what was going on right away. Despite the swift response from CMC, it was too late to mitigate the damage. "It affected numerous systems within our organization, and it affected our ability to be open," said Zlatic. The systems were compromised to the point where multiple CMC facilities would not be able to operate in a safe and predictable manner. "We, as a museum, are more complicated from a systems standpoint than I think the general public would expect us to be," mentioned Zlatic. "Complicated in a good way – we have up-to-date systems – but it means that you have to be that much more diligent…these systems are connected and need to be cleared in order to make us run."

"It affected our ability to be open."

– David Zlatic, Chief Technology Officer of CMC

CMC's IT department was able to swiftly identify the scope of the issues within their modern and complex system. "We made the decision early on to act with an abundance of caution and assume that everything was compromised," said David Zlatic. "We wanted to mitigate as much risk as possible." Zlatic's team knew their business well and were able to make the Museum Center hum daily, but in this moment of crisis they simply lacked the staff to get things back up and running safely and quickly. Indeed, time was a factor; the Museum had a hard time finding a partner who had the necessary expertise and were able to act quick enough to get the Museum up and running again. "We needed people who had done this before…there were things that were outside of our knowledge base," determined Zlatic.



THE SOLUTION

For over twenty years Atomic Data has tackled an endless variety of technology and cybersecurity projects for their clients. From their headquarters in Minneapolis, Minnesota, Atomic Data provides high-end IT as a Service (ITaaS) to companies of all shapes and sizes across the United States. Atomic Data had built a reputation in Cincinnati via the work done for Major League Soccer (MLS) club FC Cincinnati and its newly built TQL stadium. So, when David Zlatic was referred to Atomic Data by a vendor, they were able to get boots on the ground right away. With these kinds of projects, it's not uncommon for there to be issues arising daily – this network remediation was no exception. Near-constant meetings and communication were necessary. What's more, Atomic Data's engineers didn't yet know the Museum's architecture – they came in blind and had to get up to speed on the fly.

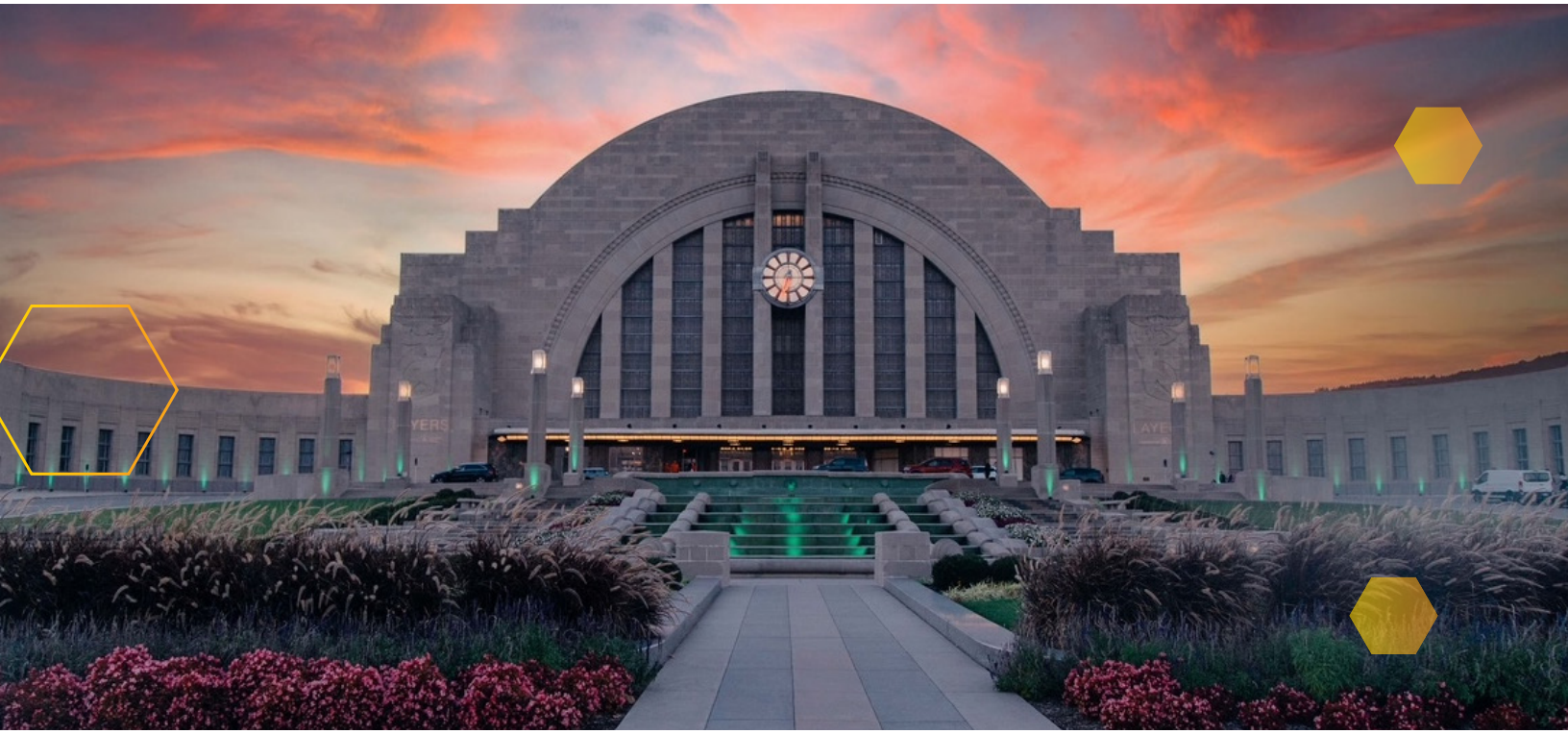
From day one, Atomic Data's engineers got to work, outlining an airtight plan to migrate Cincinnati Museum Center's networks from compromised environments to secure ones. The migration had to be all-encompassing – Atomic Data worked hand in hand with the CMC's IT group to apply security patches to all network equipment. "I was amazed… [Atomic Data's] engineers took leadership from the moment they touched down…helped us move to a restored environment" he chimed. "You don't see that all the time in the IT world."

The work didn't stop there. It wasn't enough for Atomic Data and CMC to get things back up and running – they wanted to ensure that this kind of event never happens again. Atomic Data identified a list of network device credentials that didn't meet complexity requirements and made recommendations in line with security best-practices. Atomic Data's engineers then worked to update all network infrastructure interfaces between the pertinent firewalls and switches, in addition to constructing new interfaces where it was possible. Then, Atomic Data helped put together a migration schedule.

Existing networks and VLAN configurations were thoroughly reviewed and analyzed by forensics experts to ensure that they were properly sanitized. From there, Atomic Data and Cincinnati Museum Center could begin to turn up the environments for all CMC locations in a secure fashion. It wasn't just Atomic Data's technology expertise that helped get this done. Atomic Data's engineers can excel because they're supported by a team of masterful project managers who have years of experience taking on tasks just like this one. The project managers identified key agenda topics for each meeting, determined risks and issues, flagging all dependencies, and kept a close eye on time utilization to ensure costs remained in line with client expectations.

> **"We needed people who had done this before."**
>
> – David Zlatic, Chief Technology Officer of CMC

For CMC, Atomic Data was a difference-maker from day one, helping the organization turn back up safe and sound. "It sounds like a cliché" recalled Zlatic. "But for us, Atomic Data really was a match made in heaven."



THE NEW REALITY

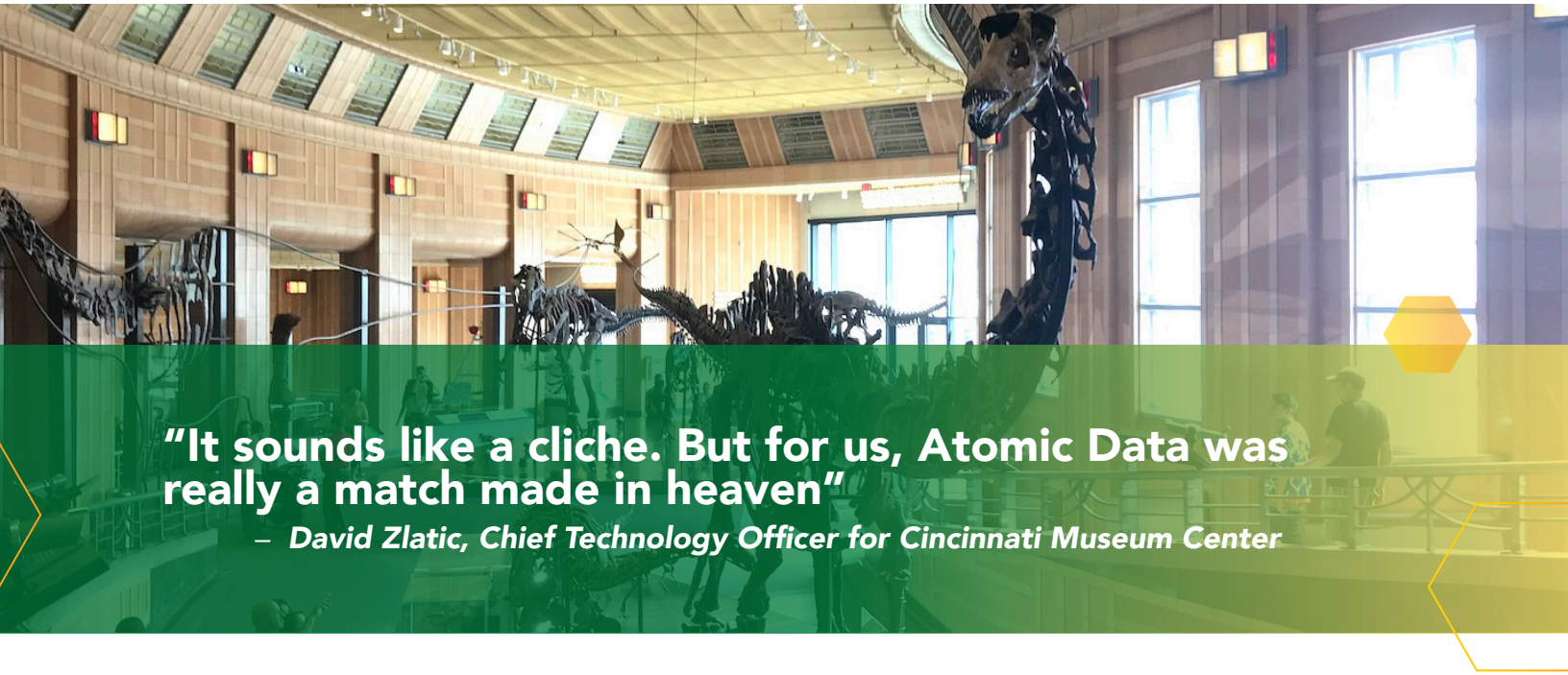
Atomic Data's support of Cincinnati Museum Center continued after they got back up and running. After the migrations were completed, a comprehensive network architecture review was conducted, where Atomic Data's engineers made future-state recommendations for the support, maintenance, and monitoring of all network devices. That was coupled with 24x7 Atomic Monitoring and the ever-vigilant eye of Atomic Data's Network Security Operations Center (NSOC). The NSOC is a proactive team of network professionals tasked with constant monitoring of all client networks. They're the first line of defense when it comes to incident response, triage, and remediation. The NSOC's constant presence ensures that CMC's IT infrastructure is under around-the-clock surveillance and care. To ensure things were buttoned up, Atomic Data's engineers deployed thorough vulnerability scans every month, compiling reports to be analyzed by the security and compliance team. These reports provided CMC with a robust security baseline, used to maintain a Vulnerability Management Program, something that's often a requirement of today's demanding insurance and regulatory environment. Ultimately, the difference is night and day. Cincinnati Museum Center has a cutting-edge security posture that ensures business continuity. "At the end of the day, we came out better," said Zlatic. "Money well spent."

CONCLUSION

That was the start of a continuous and symbiotic partnership that Atomic Data and Cincinnati Museum Center built since the incident. "Atomic Data helped us make the right steps, in terms of sequencing moving forward…and helped us build the environment we are supposed to have in the future," recalled Zlatic. Ultimately, one of the things that Atomic Data's constant presence allows CMC to do is simply, focus on business goals. "Things run more smoothly. They stay patched, they stay up to date…[this] allows us to focus on more strategic stuff instead of the nuts and bolts."

Contingency is the name of the game, as far as David Zlatic is concerned. "More than anything, what we've gained is a modern IT infrastructure…and the knowledge that somebody on [Atomic Data's] team is going to have the answer for us."

"I feel like Atomic Data, as a managed service provider, is always looking out for our best needs," concluded Zlatic. "It's truly a partnership."



"It sounds like a cliche. But for us, Atomic Data was really a match made in heaven"

– ***David Zlatic, Chief Technology Officer for Cincinnati Museum Center***

Ready to have a conversation about your security posture?

GET PROTECTED - CONTACT AN EXPERT

ATOMICdata

250 Marquette Ave, Suite 225, Minneapolis, MN 55401 | 612.466.2000 | 1.800.285.5179
atomicdata.com