tenable.ad™ active directory

CASE STUDY

LION

OVERVIEW

Lion, a subsidiary of Kirin, is a leading beverages company based in Australasia, with fast-growing operations in the United States. The company creates, produces, markets, sells, and distributes alcoholic and non-alcoholic drinks around the world. The Australia, New Zealand and US brands span beer, seltzer, wine, spirits, and coffee.

BUSINESS NEEDS

Lion needed a way to obtain visibility into the Active Directory environment to ensure that its security was being properly managed. They required actionable remediation advice and a means to measure security as it changes over time, whether due to improvements made by the team or the natural deterioration of controls.

Industry: Food & Beverage

Location: Australia, New Zealand and the US

Revenue: $1.53B

Products used:

tenable.ad™ active directory

Results:

- Visibility of the Active Directory architecture enabled the team to eliminate unused domains, thereby reducing the attack surface.
- Remediation advice specific to their environment saves the team time and effort.
- A security posture score fosters a culture of continuous improvement.
- Leadership can validate that the environment is being properly and securely managed.
- Proactive, preventative Active Directory hardening measures to protect against future attacks.

CHALLENGES

When Jamie Rossato joined Lion as Information Security Director in January 2021 his responsibilities were clear.

"I was charged with driving a comprehensive cybersecurity investment program to ensure that we have effective governance and management over our information and our data," says Rossato.

In addition to overseeing information security, Rossato serves as the privacy officer for the leading global beverage company. His scope includes Australian and New Zealand operations directly, as well as the brewery lines of business in the U.S. He is accountable for both IT and OT security.

When he joined Lion, one of Rossato's top priorities was implementing Tenable.ad. "I wanted to grasp the configuration of our Active Directory environment and work on a program to address our security needs," he explains.

Like most organizations, Lion had an opportunity to enhance security in the Active Directory environment. "An organization's security posture for Active Directory deteriorates over time, and requires ongoing focus to ensure secure configuration within Active Directory," says Rossato.

SOLUTION

Rossato knew, from previous experience with the tool, that Tenable.ad would enable him to understand the security posture of the Active Directory environment and determine whether it was being properly managed. "We needed an appliance or a control that could independently but continuously provide visibility of what our Active Directory configurations look like," he says.

The complete visibility provided by Tenable.ad allowed Lion to make immediate improvements, beginning with the architecture. The Active Directory consisted of a forest with three domains, one of which had a sub domain and was the only one being used. The two that were not being used were removed, leaving the organization with a single domain and subdomain. This immediately reduced the organization's attack surface while improving its overall risk posture.

The team also made immediate improvements in performance. They could see failed logins, including scripts with credentials that were failing and, as a result, causing performance issues. Because the team could see that the scripts themselves were broken, they could confidently turn the scripts off without the fear of causing something to break.

RESULTS

Tenable.ad was able to identify security issues present in the environment. "Tenable.ad very quickly gave us visibility into Active Directory, including the actual configurations and misconfigurations that were in place. We got a clear risk lens and action plans to remediate security issues, which allowed us to set up the program of work that we've been on ever since," he says.

Because Tenable.ad provides remediation advice that is specific to Lion's environment, the infrastructure team understands both what to fix and exactly how to fix it. This eliminates the need to research how to resolve an issue as well as the temptation to ignore it. "You're able to improve the security of your AD environment and educate the team that's meant to support it, which is one of the unspoken benefits of Tenable," Rossato says.

Tenable.ad also assigns a score to the Active Directory security posture, allowing Lion to measure security over time. Rossato established a posture target for the AD team, empowering them to make the necessary changes to achieve it. By tracking progress against the score, team members were motivated to not just meet the target, but stretch themselves to further improve the security score. "With Tenable.ad, we can go on that journey of continuous improvement and keep pushing up the bar of performance."

With the visibility provided by Tenable.ad, everyone knows exactly what to do to get there – as well as how far they've come. "We have substantially improved the security set up of our Active Directory with Tenable.ad," says Rossato. "It's an excellent tool. Whenever a CISO asks me what tools we're using that deliver value, I tell them Tenable.ad."

Learn more: www.tenable.com/products/tenable-ad

About Tenable

Tenable® is the Exposure Management company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com.