CASE STUDY

tenable Identity Exposure

HOW A GLOBAL MANUFACTURER MITIGATES MISCONFIGURATION RISKS IN REAL-TIME WITH TENABLE IDENTITY EXPOSURE

vallourec
SMART TUBULAR SOLUTIONS

OVERVIEW

Vallourec is a multinational industrial company headquartered in Meudon, France. The Group is a world leader in premium tubular solutions for the energy markets and for demanding industrial applications such as oil & gas wells in harsh environments, new generation power plants, challenging architectural projects, and high-performance mechanical equipment. Vallourec's pioneering spirit and cutting edge R&D open new technological frontiers. Today, the company has close to 17,000 employees in 20 countries.

BUSINESS NEEDS

Industry: Oil & Gas Manufacturing Company

Location: Worldwide

Size: 17,000 employees

Revenue: 3.4billion €

Solution

tenable Identity Exposure

Results

- Complete visibility of AD infrastructure
- Real-time detection of misconfigurations, eliminating the need to manually run scripts
- Live monitoring allows the team to see the impact of infrastructure changes in real time
- Controls preserve configurations to maintain good security hygiene

CHALLENGE

Like the majority of enterprises, Vallourec relies on Microsoft Active Directory for authentication and authorization. Also like many enterprises, the manufacturer recognizes the need to secure this mission critical IT asset. However, despite the security team's best efforts, misconfigurations were continuing to expose the organization to risk. The team needed a way to monitor Active Directory and be notified of changes in real time so that it could remediate security issues before they became a foothold for threat actors.

Vallourec's Active Directory supports 17,000 global employees. Management of the system is decentralized. "We have groups moving fast, and security is not the first thing admins think about when a boss is demanding a new solution be installed. Sometimes they make mistakes," says Jeremie S., an Active Directory architect at Vallourec.

Those mistakes, if not identified and remediated, could be costly. Active Directory is a favored attack vector for bad actors who use its misconfigurations to move laterally across systems and escalate privileges. It is critical to catch misconfigurations early to reduce security risk and to prevent further misconfigurations.

The team was using scripts to manually check for misconfigurations, but the process was slow, and the team knew it wasn't seeing everything. "The admins do things that we couldn't even imagine. It may be evident to us that we don't do it that way but for them, it can make sense during the implementation of a product," says Gerald S, IT and Active Directory and Identity Architect at Vallourec.

These manual checks were performed periodically, allowing admins to continue to build off of misconfigurations and making them more difficult to fix when they were spotted. The team wanted to monitor Active Directory and track changes in real time, as well as restrict admin rights based on the operations they perform.

SOLUTION

Vallourec chose Tenable Identity Exposure (formerly Tenable.ad) to obtain the visibility and control it needed to effectively secure Active Directory. Tenable Identity Exposure enables the team to see every change in Active Directory, determine their risk level and exposure in real-time, and prevent attackers from using AD as a critical attack path.

The manufacturer worked with its managed SOC provider to integrate Tenable Identity Exposure into its SIEM. This involved simply opening a port and defining a target IP. Upon implementation, the team immediately noticed an improvement in the visibility it had of the AD infrastructure. *"When we first installed Tenable Identity Exposure, we had some security misconfigurations that we hadn't detected before,"* says Gerald S., IT and Active Directory and Identity Architect at Vallourec.

About Tenable

Tenable® is the Cyber Exposure 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.

RESULTS

The team fixed those misconfigurations and is now automatically notified when Tenable Identity Exposure detects a change in Active Directory. "We can ensure that everything that we want to configure in terms of security or exception is still in place and no one can change it, not even us. If someone has the right to change something, we can see it directly. In fact, it's a real time supervisor for me on the direct configuration," says Jeremie.

The team is no longer focused on writing and running scripts to detect misconfigurations, and the time it does spend on fixing misconfigurations is greatly reduced. "We can capture the bad configurations quickly. One fix now, which takes five minutes, used to take five days or five weeks if the configuration had been replicated and we needed to make a lot of changes," says Ben P., team lead for the infrastructure operations team.

One of the team's favorite features is Trail Flow, which displays the real-time monitoring and analysis of events affecting the AD infrastructure and allows teams to identify critical vulnerabilities and their recommended courses of remediation. When new features are introduced to Active Directory, Trail Flow allows the team to see how those features impact the infrastructure. The team can also see fake authentication attempts, where around the world they're originating from and whether they're due to a misconfiguration problem or simply a problem on a domain. This visibility allows the team to drill into root cause and more efficiently address the issue.

The team also appreciates the Tenable Identity Exposure dashboard, which allows them to track alerts and see the evolution of their security efforts. Tenable Identity Exposure has given the team the visibility and control over Active Directory that it couldn't otherwise achieve. "We wouldn't be able to mirror what Tenable is doing and make it viable. It does the job it needs to do, and it does it well," says Ben.