CASE STUDY

tenable.ad

How global manufacturer Somfy monitors and protects its Active Directory infrastructure

Establishing continuous monitoring and security of directories

- Industry: Access Control Systems Manufacturing
- Location: France
- Revenue 2020: €1,257.1M

somfy

Founded in France in 1969 and present in 58 countries, Somfy is the leading partner in all areas of building opening automation systems and a pioneer in the connected home sector. The group is constantly innovating to create homes that offer their users comfort, well-being, and safety to fulfill its vision of "inspiring a better way of living accessible to all."

This is achieved through five applications and a portfolio of 13 complementary brands:

- Shutters and solar protection
- Interior blinds and curtains
- Connected home
- Security
- Access control

The entrepreneurial spirit of Somfy is embodied by the Group's 6,070 employees in 117 subsidiaries, eight manufacturing plants, and 80 logistics centers and warehouses. Its presence on five continents enables the group to adapt its products and services to the specific needs and characteristics of its markets.

By capitalizing on digital technology, innovation, and partnerships, Somfy is perpetually renewing its value proposal for all its stakeholders.

Benefits

- Continuously monitor in real-time to discover weaknesses and misconfigurations
- Continuously refine remediation and mitigation plans

KPIs

- 2 domains
- 1 Forest

Stakeholders at Somfy

- 3 Active Directory Administrators
- 1 Security Manager

Tenable.ad dedicated team

- 1 Tenable.ad Technical Account Manager
- 1 AD Advanced Security Engineer

Challenges

As a global player in home and commercial control systems, Somfy aims for the highest levels of innovation and advancement in its products and solutions. With several companies under its umbrella, Somfy's security for intellectual property, design, and customer data spanning a vast directory infrastructure was paramount. As a part of its continuous improvement process, Somfy was seeking the best way to tackle unique AD security challenges. This required a targeted assessment of the root domain to identify any issues.

Identifying Existing Weaknesses

Utilizing Tenable.ad for AD's seamless, instant-on deployment, Somfy was able to immediately investigate and identify problems in real-time, each corresponding to one of Tenable.ad's Indicators of Exposure (IoE). Some of the major issues were related to the indicators AdminSDholder, Root Permission, and Kerberos Delegation. The results from the initial AD assessment highlighted too many administrators across numerous groups.

This initial connection between Tenable.ad and Somfy's AD was vital, as the solution mapped the AD's topology and identified any existing hidden attack pathways and weaknesses that could be leveraged by attackers.

Child Domain Complexity

After the initial connection and analysis of the root domain, attention turned to the child domain. However, a few challenges with the child domain showed potential loopholes and vulnerabilities. These included:

- Many entities in numerous global locations
- Many AD administrators
- Several administrators coming from outsourced, third-party resources

Solutions

Following the initial assessment exploring existing weaknesses, misconfigurations, and attack pathways, the Tenable.ad solution provided step-by-step remediation tactics to prevent vulnerabilities and attacks. Due to Somfy's need to quickly acquire some additional expertise relating purely to AD, Tenable.ad's reputable partner provided ongoing workshops to analyze each IoE. The partner organized a tailor-made mitigation plan based on Tenable.ad for AD's real-time results available to Somfy senior staff through an intuitive, consolidated dashboard.

Thanks to the Tenable.ad platform's consistent real-time AD monitoring, Somfy was able to perform continuous workshops to address each actionable IoE task, while relevant teams were equipped with Tenable.ad-proposed checkers to ensure each step was mitigated. A workshop was set up for each IoE according to complexity and helped teach Somfy how to maximize the Tenable.ad solution.

Once the mitigation steps were complete, Somfy's security team cross-referenced via the Tenable.ad platform to check the security status. Somfy was able to monitor its own compliance standards for AD, continuously monitor AD, and even receive assistance to establish compliance rules.

This method of measuring AD security achieved quick wins for the security team. Once the mitigation steps were complete, monitoring of the root domain continued to safeguard the Active Directory. Following this, the child domain was addressed.

"I NEEDED A TOOL WHICH WOULD TALK TO ADMINISTRATORS SO THEY WOULD DEVELOP THEIR SECURITY AWARENESS AND BECOME SO TALENTED THAT THEY WOULDN'T CAUSE ANY NEW DEVIATIONS. TENABLE.AD'S DASHBOARDS, ALERTS, AND SEARCH CAPABILITIES FIT THAT PURPOSE ENTIRELY."

– Didier Cambefort
CISO

Result

- An adequate delegation model was put into practice to avoid the use of built-in privileged groups.
- New security issues introduced by AD admin misbehavior were identified and mitigated within one day.
- Systems and jobs configured with wrong credentials were spotted and located by the brute-force detection; their misconfiguration was fixed.
- A tweak in the domain configuration ensured that newly joined machines fell under the security patching GPO.
- Many service accounts were reconfigured to reduce their capability to damage the domain.