tenable.ad™

CASE STUDY

Protecting Directories and Defining Threats in the Insurance Sector

- Industry: Insurance
- Location: France
- Revenue 2018: €253M

GROUPE PASTEUR MUTUALITÉ

Founded in 1900 and headquartered in Paris, Groupe Pasteur Mutualité (GPM) is a French insurance company providing mutual insurance and services primarily for healthcare professionals. GPM emphasizes innovation, prevention, and solidarity at the heart of its development projects and its strategic plan, GPM#2022. Recently, GPM has built a new health center and services for healthcare professionals called Villa M – Paris.

Currently, Groupe Pasteur Mutualité protects 180,000 people, has 138,000 members, and has 500+ employees.

Challenges

Limited resources for AD security

Groupe Pasteur Mutualité's security structure was stretched, with limited resources and person-power dedicated to securing Active Directory. A small IT team held responsibility for company-wide cybersecurity ranging from endpoint protection to access

KPIs

- 1 Domain
- 1 Forest

Stakeholders at GPM

- 5 AD Admins
- 5 people for support

Tenable Dedicated Team

- 1 Technical Account Manager
- 1 Engineer
- 1 Customer Success Manager

Benefits

- Intuitive security dashboard providing deep AD insights
- Real-time, continuous identification of weaknesses and misconfigurations
- Successful integration with SOC environment

management and beyond. However, this lack of expertise did not compromise their prioritization for AD security, and the company recognized the importance of Active Directory as their centralized zone for user credentials, authorization, authentication, company systems, and more. Since 2020, a major cybersecurity program has been implemented, including substantial remediation of Active Directory and dedicated use cases concerning threat prevention.

No visibility for AD security

One of their principal concerns was the underwhelming lack of visibility into Active Directory to properly analyze any weaknesses and vulnerabilities that may occur. Equally critical would be maintaining the security level and, if ever necessary, initiating AD remediation actions. However, it was also important to first establish the security state of AD at that point in time. IT systems and security outsourced and managed by a third-party organization were major factors that contributed to reduced visibility. The already limited resources for AD security were further strained as the team's responsibilities widened. This change created the need for Tenable for AD to provide agentless, continuous AD monitoring and proactive security.

Solutions

The Chief Information Security Officer spoke with Tenable specialists during France's premier cybersecurity conference, "Les Assises de la Cybersecurité". He was astounded by the seamlessness and simplicity experienced during the solution demonstration. The CISO further participated in CESIN* special training, "Paroles d'Experts", where Tenable's founder explained Active Directory security. In a follow-up workshop, GPM agreed to proceed with a preliminary Proof of Value (PoV) stage to identify the current state and health of the AD. Via the initial PoV, GPM was able to immediately discover, map, and score all existing weaknesses and misconfigurations. With the Tenable platform delivering deep insights into the AD hygiene, GPM opted to engage with the Tenable team and establish a truly proactive AD security program that protects admin credentials and service account credentials. Monitoring would ensure limited groups or users have DC admin rights plus mitigate AD attacks.

*CESIN is a French think tank specialized in cybersecurity insights

Following the successful PoV, the immediate objectives included:

- Checking existing AD configurations
- Initiating all AD remediation actions in an efficient, timely manner
- Integrating external Synetis team to analyze and identify critical actions
- Integrating IT colleagues to optimize knowledge on all AD concepts
- Maintaining compliance score at a consistent level 3
- Initiating use cases for the SOC environment, with SIEM integration
- Integrating SOC teams into an alerting process
- Integrating email alerting for remediate configuration actions
- Investigating and visualizing activity/objects in real time via trail flow

Result

- Remediated Indicators of Exposure (IoE) identifying all weaknesses
- Understood the global AD configuration and objects
- Exposed how a misconfiguration or weakness can be exploited by malicious actors
- Identified any weaknesses and discovered persistence tools
- Prioritized actions to remediate big security gaps
- Implemented real-time email alerts when IoE triggers are activated
- Identified and reported the relevant KPIs in a global dashboard for senior management
- Defined a global plan for threat prevention, based on five use cases
- Set up the alert chain with the SOC team
- Integrated SIEM with the Tenable platform to immediately remediate relevant actions
- Configured IoE
- Tested sandbox and production environments
- Correlated Event Windows with SOC teams
- Visualized all notifications on the SOC dashboard

“Tenable.ad is a pragmatic solution that allows our teams to obtain the necessary visibility and prioritize actions for Active Directory remediation. My goal is to discover any weaknesses and to activate real-time alerts. Thanks to dedicated use cases on threat prevention, all stakeholders are mobilized, which makes the remediation process faster. Big picture: it’s easier to report the relevant information in a global dashboard for senior management. We directly identify the most important actions, and we raise the global compliance score.

The next step for Groupe Pasteur Mutualité is to implement a new unique plan focused on threat and attack detection.”

- GPM, CISO