

A Structured Approach to Secure the Next Uncharted Minefield with an SAP Assessment

About the Customer:

Altán Networks is one of the largest telecommunications conglomerates in North America. Securing the S/4HANA-System is mission-critical to reach the company's business objectives: To cover at least 92,2% of the Mexican country with 4.5G services.

The Challenge:

Altán Networks has various external service providers who host and manage the existing SAP environment. The responsibility to safeguard critical applications like SAP was non-negotiable for José Márquez, CISO of Altán Networks. Due to his career path he has an advanced understanding of both worlds - SAP and Cybersecurity. Understanding the existing attack surface in SAP and establishing an effective security strategy covering people, processes, and technology was the challenge ahead.

"SAP Security can be a minefield for the reactive organisation. To reduce risk and safeguard our crown jewels, we have to think 'end-to-end' and be prepared to step outside the lines of boxed-in thinking. We practice a continuous, proactive approach to securing SAP applications based on processes, technology and people."

Dipl.-Inf. José Márquez
CISO at Altán Networks

Our Strategy:

Aligning the SAP and security team to gain a common understanding of responsibilities and required skills is fundamental to implementing a security strategy. By applying the NO MONKEY Security Matrix in technical assessments and subsequent workshops, we identify security white spots and critical vulnerabilities in a comprehensive way aligned with the SAP Security Maturity Model. Thus the management of findings is approached collaboratively by identifying and addressing their root causes.

"Customizing services around an organisation's security requirement is an approach that has been effective to find the appropriate protection measures across people, process, and technology."

Waseem Ajrab
Head of Advisory at NO MONKEY

Our Solution:

Customising an SAP assessment around the business requirements and objectives of Altán Networks enabled us to provide a holistic overview of the different pain points around their SAP environment. While other service providers might concentrate on protecting the technology of SAP alone, we ensured that all the critical assets (people, process, and technology) are included. Our holistic approach didn't only stop there but also made sure that a continuous protection plan was provided and aligned with the entire organisation's security objectives and requirements.