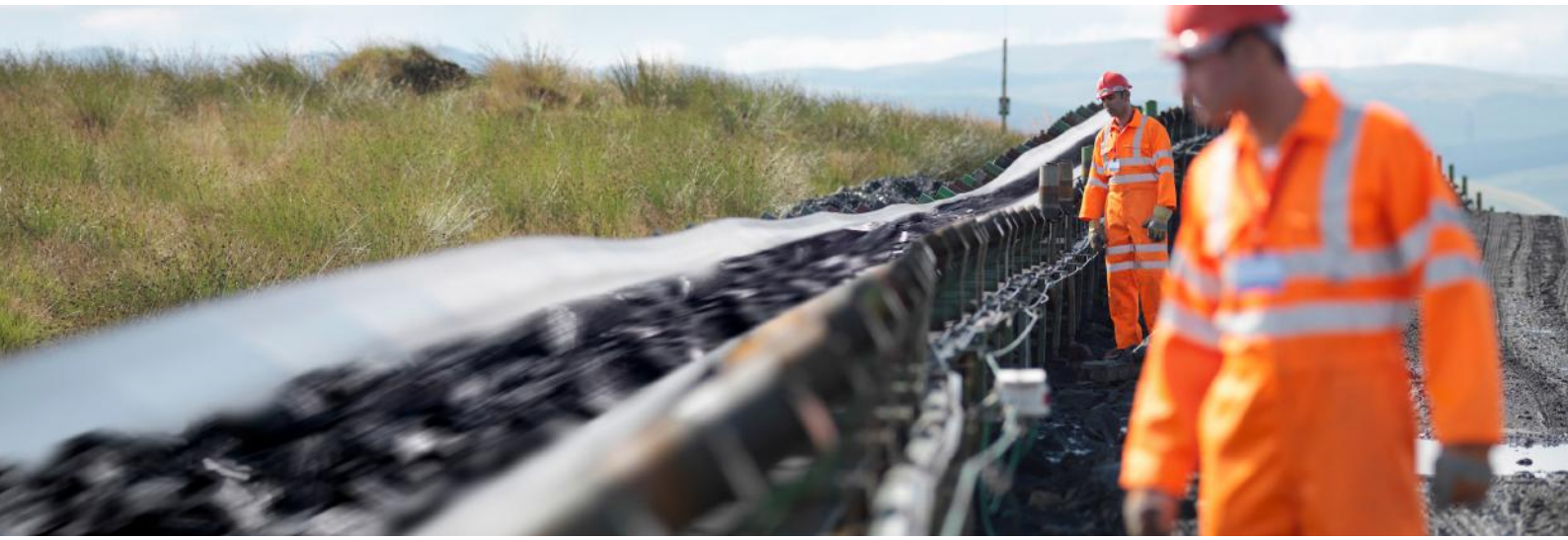
Orange
Cyberdefense

Customer stories

TAL Cyberdefence for the transalpine pipeline



At a glance

- Branch: Petroleum Industry
- Formed: 1965
- Services:
- Analysis and strategic consultancy on a security plan
- Implementation of a SIEM
- Implementation of an Intrusion Detection System
- Implementation of an Asset Management Plan
- Integration in an existing complex system landscape
- Achieving ISO 27001 compliance

Pipeline across the Alps – carrying oil and data

The Transalpine Pipeline is one of Europe's most important pipelines. It is one of Germany's four central oil supply lines. The pipeline covers a length of 465 kilometres, from Trieste to Lenting, close to Ingolstadt, and then a further 287 kilometres all the way to Karlsruhe. It also conveys over 40 million tonnes of crude oil across the Alps each year.

The infrastructure for the logistic and organisational operation cannot be underestimated: starting with storage tanks in Trieste and Lenting, via ten pumping stations to an oil pipeline power station unique in the world, which – just as with a hydro-electric power station – recovers energy from a downhill run.

The pipeline is monitored from two control centres in Trieste and Lenting. In Germany, the Deutsche Transalpine Oelleitung GmbH is responsible for operations.

Owing to its significance in the energy supply chain, the TAL has been classified as critical infrastructure (KRITIS). Consequently, it was essential that the safety systems also underwent a thorough inspection as part of cyber defence.

Composition of a strategic security infrastructure

From the outset of the project, individual components such as a firewall and endpoint protection were already available. However, in order to be equipped for the future and to increase the security level efficiently, a wide-ranging strategic approach was needed.

At the same time, a critical factor was that IT has traditionally been kept "lean and mean". Outsourcing was consequently a fixed core component of the strategy.

To take this into account, a solution concept was also polled which rested primarily on

highly automated solutions and managed services. In addition, a seamless integration into the existing systems was also a part of the requirements, as was good modularity and ease of expansion.

With KI and MSS support in the future

In advance, there had already been good contact with project partners. Those in charge had the opportunity to brief themselves at technical events on the solutions offered by Orange Cyberdefense and could even cast an eye behind the curtains at one of the regularly held CDC viewings of Orange Cyberdefense's five operating cyber defence centres.

Orange Cyberdefense's plan was finally persuasive through the successfully enacted POC: A conclusive mix of intelligent managed services and easily automated and partially KI-based tools provided an insight. Processes in the network could be recorded exactly and made visible. This facilitated a timely recognition of security issues effectively at an early stage.

ISO 27001 certification was supported by the integrated security solution.

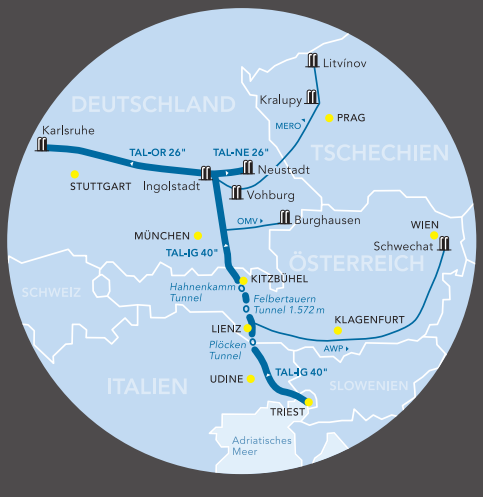
Implementation was completed quickly and without complications from the customer's perspective: After a pilot phase lasting a mere two weeks, it was possible to change to a productive operation.

Early successes even in the pilot phase

The advantages of the solution implemented by Orange Cyberdefense were obvious even during the introductory phase: Two security incidents were simulated and these were detected and fended off successfully.

Not least because of the smooth project implementation and excellent performance, expansion of the project is now planned to sites in Austria and Italy.

"We value the efficient working methods and excellent expertise from our collaboration with Orange Cyberdefense Germany. Orange Cyberdefense is a service provider who understands us and implements our requirements in detail. The implementation was a great success!"



About Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense, Uilenbaan 80, 2160 Wommelgem | T: +32 (0)3 641 95 95 | info@orangecyberdefense.com | www.orangecyberdefense.com/be