

CASE STUDY Banking Institution

Supervision of internal network – Ensuring the security of users and selected services



Komerční banka, a.s. is a **leading banking institution in the Czech Republic**, Central and Eastern Europe and part of the international Société Générale Group. This bank institution has been providing **retail, corporate and investment banking services** since 1990.

As a key banking institution, the client has been a long-term user of a wide range of security solutions to keep pace with the increasing demands on its IT infrastructure's security. The next step to increase security was to select a **product for internal network monitoring**. For this reason, Komerční banka, a.s. launched a tender in which we and our partner were successful with our GREYCORTEX Mendel product.

Challenges

The main requirement was to **secure the bank's headquarters** along with providing classic user security.

The security department is made up of dozens of people at different security levels whose task is to **secure the backbone network** of the bank's data centre. All branches are connected to it, while the backbone network includes thousands of subnets containing tens of thousands of devices.

Therefore, it is **crucial** for the customer **to ensure the visibility of all devices** in the subnets and **verify compliance** with the bank's security policies.

Results

GREYCORTEX Mendel provides the security team primarily with **visibility into the network**. It detects and clearly displays who is accessing what and where and the access they have – for example admin access to remote device management, a VPN or internal network activity and access. Using deep visibility into the network, Mendel also provides classic user security.

Before deploying the new technology widely in the bank, there was a long-term testing phase in the internal environment. This two-year period was successfully completed and the next phase of deploying the solution to other network segments is currently underway.

The customer cites its **ability to work with historical data** as being the main advantage over the previous solution. That, among other things, improves the quality of machine learning, thereby strengthening general network protection and real-time threat detection. This gives the security team unique visibility into the network, even in the context of time – they can see who is accessing where today and what accesses existed in the past.

The bank now has a dedicated team working with GREYCORTEX Mendel. They specify individual use cases, as required, and configure the Mendel solution specifically for use in these cases.

The customer's security team plans to expand the use of Mendel gradually for other specific purposes, and will work with our cybersecurity experts on this as well.

Situation

- A large number of subnets for different purposes (for testers of new applications, for penetration tests, etc.)
- A variety of users and permissions for accessing different parts of the network

Customer requirements

- Need for deep visibility into the network and subnets
- Require control of security policies within user networks

Results

- Detailed visibility of a large number of subnets in real time
- Can view and analyze historical data in the context of a given event
- Customization of GREYCORTEX Mendel to meet the needs of the security team
- Security policy validation, including subnet access settings