CaseStudy

Cyber Operations Center of the South Moravian Region

Due to a growing number of cyber incidents, including several publicized ones, the South Moravian Region decided to introduce additional security measures. Based on an internal analysis, its Cyber Operations Center concluded that ESET's Endpoint and EDR solution was the right tool for increasing cybersecurity and detecting cyber attacks early on.

KYBERNETICKÉ OPERAČNÍ CENTRUM

INDUSTRY
IT security, public sector

WEBSITE
www.kr-jihomoravsky.cz

COUNTRY
Czech Republic

PRODUCT
ESET Inspect,
3000 seats

THE CUSTOMER

The Cyber Operations Center (KOC) is a department integrated within the Director's Office of the South Moravian Region. Its task is to centrally monitor and evaluate possible cybersecurity threats in the regional office networks and affiliated contributory organizations. This brings several advantages to the South Moravian Region and the organizations, thanks to allocated professionals dealing with security threats across the network, information sharing among these entities and implementing effective measures in the shortest possible time. The Cyber Operations Center is the first to successfully implement a project of this kind at the regional level.

THE CHALLENGE

The main challenge could be summed up by the words *"you can't control and can't fight what you don't see,"* says Aleš Staněk, Head of the KOC department.

KOC needed data sources providing detailed information on the behavior of computers and servers in the individual organizations. The end stations and servers were another vital element of this security puzzle. At the same time, the administration of the antivirus solution had to remain in the hands of the organizations, and the EDR solution couldn't intervene with the existing operations in any way.

"It wasn't just about collecting information. We needed to have the ability to respond to security incidents actively. This was another key requirement for the needed EDR solution." adds Staněk.

THE SOLUTION

ESET Inspect provides KOC with additional data needed for the work of security analysts. KOC then evaluates it in the SIEM tool in the context of information from other sources (operating system, firewall, network probe, etc.). *"Thanks to the data from ESET Inspect, we know almost immediately about the security incident, and we can react to it promptly,"* explains Staněk. Thanks to the solution, KOC can take active steps in cooperation with the organizations to stop a potential infrastructure compromise, for example, by isolating the suspect computer from the network until the incident is investigated.

IMPLEMENTATION

ESET, in cooperation with AXENTA, a.s., divided the project into two phases—implementation and optimization.

Implementation process

The main advantage of the ESET Inspect is the simplicity of its deployment in an environment where ESET security products are present, including central management. The implementation consisted of two steps - server deployment parts and ensuring the distribution of EI agents. *“ESET’s EDR solution has been deployed in approximately 3,000 terminal equipment in 11 separate organizations. Despite such a large number of stations and different infrastructures, we managed the implementation within 4 weeks,“*describes Lukáš Přibyl, CEO of AXENTA. The deployment was time-consuming due to the alignment of the schedule with all individual organizations. After reassuring them that there are no conflicts with their environment, we have moved to the second, optimization phase.

Optimization or looking for a needle in a haystack

The optimization phase of the project was even more challenging, primarily because there were 11 different networks. This phase included three major steps:

- the creation of a universal ruleset for a hospital environment,
- its distribution to all organizations,
- adjusting the sensitivity of the rules depending on the specific environment.

To streamline the optimization phase, an API server was used for mass distribution of the rules, and fine-tuning took place via the Enterprise Inspector web interface. *“We were able to handle the initial optimization in all organizations within three months,”* adds Přibyl. However, it should be added that due to the high sensitivity of the ESET Inspect solution, the optimization part is a continuous process because each newly introduced application in the organization’s environment can show unexpected behavior that needs to be revised.

NETWORK VISIBILITY AS A KEY TO PREVENTION

ESET Inspect helps detect anomalies and errors of varying severity. *“It was usually bad configuration networks or improper application settings that could, in extreme cases, lead to security incidents,”* explains Aleš Staněk. Based on the identified shortcomings, the KOC continuously provides recommendations for adjusting security policies and application settings in the organization. *“Valuable information from ESET Inspect has become an integral part of addressing most potential security issues incidents. It thus provides us with additional information to illustrate the context of the event, which we have not had before,”* he concludes.

KEY BENEFITS

○ Easy deployment
○ Active response and early detection
○ Outstanding network visibility

Digital Security
Progress. Protected.

ESET is a leading IT security company from the European Union with its headquarters in Bratislava, Slovakia. The company, which was founded in 1992, has a global presence and now protects 110 million users and 400,000 businesses worldwide. **www.eset.com**