SUCCESS STORY

SBA Research gGmbH

Programme: COMET – Competence Centers for Excellent Technologies

Programme line: COMET K1

Project: Networked Systems Security

HIGHER EFFICIENCY AND SECURITY IN LARGE NETWORKS

ANOVIS AND SBA RESEARCH DEVELOP TOOLS FOR SECURE AUTOMATED CONFIGURATION IN LARGE NETWORK ENVIRONMENTS.

SIEM systems enable the central collection and analysis of security-relevant data from various sources such as firewalls, intrusion detection systems (IDS), antivirus software, servers, and applications. This provides a holistic view of the company's security situation and facilitates management and monitoring. In addition, SIEM systems are able to detect security-relevant events in real time. By analyzing log data and applying correlation rules, potential security incidents can be quickly identified, and appropriate countermeasures can be initiated to minimize damage.

SIEM systems are a central element of the MSSP (Managed Security Service Provider) services that Anovis has developed in recent years together with the experts from SBA Research. At the heart of the Anovis service model is the operations module. It is based on the ITIL process framework and comprises various services that ensure continuous operations around the clock.

SBA Research works with Anovis to develop tools that improve the automation of the numerous components. One example of this is a module that automatically rolls out the necessary configuration changes to all affected firewalls in large network environments when network components in CMDBs (Configuration Management Databases) are changed.

Markus Guttenberg, Managing Director of Anovis, describes how important such components are in a com-

Federal Ministry
Republic of Austria
Climate Action, Environment, Energy, Mobility, Innovation and Technology

Federal Ministry
Republic of Austria
Digital and Economic Affairs

lex overall system in order to handle processes efficiently, quickly, and securely: “These tools enable us to offer high-quality security services at competitive prices. It saves on personnel resources, as we can carry out complex work steps fully automatically. However, extremely broad and in-depth specialist knowledge is required for this to work reliably. Thanks to our long-standing collaboration with SBA Research, we have been able to build up this expertise and turn it into valuable tools.”

COMET - Impact and effects

In addition to various tools for the secure automation of complex network configuration changes, Anovis and SBA Research are also working on ASM (Anovis Security Monitoring), a SIEM module based on the ELK stack (Elasticsearch, Kibana, Beats, Logstash), which makes it possible, for example, to translate logs from a wide range of network components so that they can be processed centrally. Playbooks were also jointly developed, which make the daily work of analysts in the MSSP environment considerably easier and guarantee uniform quality standards in processing.

A decisive advantage of the long-standing COMET collaboration between Anovis and SBA Research is the continuous further education and training of employees. Targeted training and knowledge transfer between the two organizations ensures that everyone involved is always up to date with the latest technology and best practices in the field of IT security. This makes a significant contribution to ensuring that the services offered are of the highest quality and meet the current threat scenarios.

The joint success story of Anovis and SBA Research impressively demonstrates how the combination of research and practice can result in innovative security solutions that meet the requirements of large corporate environments. Through continuous cooperation and the pooling of expertise, Anovis is able to offer its customers customized and highly efficient security solutions that sustainably improve both the operation and security of IT infrastructures.

In conclusion, Markus Guttenberg emphasizes: “The successful partnership between Anovis and SBA Research is a prime example of how research and commercial application can go hand in hand to create forward-looking solutions. We are proud not only to be able to offer our customers first-class security services, but also to make an active contribution to the further development of the IT security landscape.”

Project-Coordination (Story)
Markus Klemen (Managing Director)
T +43 (0) 1 505 38 88
mklemen@sba-research.org

SBA Research gGmbH
Floragasse 7, 5. OG, 1040 Vienna
T +43 (0) 664 4111588
mklemen@sba-research.org
www.sba-research.org

This success story has been approved for publication on the FFG website by the center management and the project partner involved. The COMET Center SBA-K1 is funded within the framework of COMET - Competence Centers for Excellent Technologies by BMK, BMDW and the City of Vienna. The COMET program is managed by the FFG. Further information on COMET: www.ffg.at/comet

Federal Ministry
Republic of Austria
Climate Action, Environment,
Energy, Mobility,
Innovation and Technology

Federal Ministry
Republic of Austria
Digital and
Economic Affairs

Austrian Research Promotion Agency
Sensengasse 1, A-1090 Vienna
P +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at