

ISP Cyber COP

Development status

Phase 3

Technology validation and implementing it in real environment. Testing the technology outside of the laboratory and its adjustment to external conditions.

IP protection status

Partnering strategy

licensing

Institution

jctt Jihočeské Univerzitní
a Akademické centrum
transferu technologií

**University of South Bohemia in
České Budějovice**

Challenge

Protection of computer networks against hacker attacks can be ensured by various available products or services. For large data centers or other institutions, ensuring the security of these networks can be very expensive. The motivation for the development of ISP CyberCOP was to create a cheap, secure, reliable and easily scalable solution for detecting the most common network attacks.

Description

ISP CyberCOP is a probe in network traffic that can detect a problem, recognize a type of cyberattack, prevent such an attack on this network and connected devices, and alert about this situation. The system works by analyzing data passing through the computer network through the probe. It transmits information about network traffic using the IPFIX protocol to network detectors, which reveal basic types of network attacks such as port-scan, password cracking, DDOS, sending spam, etc. from the provided data and report on this to the network administrator or user. The system is based on the Apache Kafka platform designed for processing big data and allows easy and efficient scaling of the system. The solution is therefore very easy to adapt for small and large companies and Internet service providers.

Commercial opportunity

Potential users are all entities that need to protect their computer networks from network attacks. Thus, for example, data centers, Internet service providers or telecommunications companies.