

About Sycope

Sycope is focused on designing and developing highly specialised IT solutions for monitoring and improving network and application performance.

Our solutions were created and developed by engineers, who have been working on the issues of network performance, application efficiency and IT security for over 20 years. Using the solutions from global APM/ NPM and SIEM providers, they have completed more than 400 projects for such customers as Franklin Templeton Investment, The Ministry of Defense, NATO, National Bank of Poland, T-Mobile, Ikea, ING Group, Orange and Alior Bank.

In addition to many successful implementations, the team's competence has been confirmed by many individual certificates, including: personal security clearance up to 'Confidential' and 'NATO Secret' clauses, CISA, CISSP, ISO 27001 Lead Auditor, IBM Certified Deployment Professional Security QRadar SIEM, ArcSight Certificate AS Data Platform Technical, Certified Ethical Hacker, and Offensive Security Certified Professional.

This made them convinced that engineers who work in large organisations do not need a system that presents all available data about networks, devices and applications. What they need instead is selected, specific information presented as rapidly as possible. That is why the new system called Sycope has been created.

About product

Sycope is a network monitoring tool using real-time flow analysis, enriched with business context to help businesses assess performance and protect IT infrastructure. It records, processes, and analyses all parameters contained in flows, enhanced by SNMP, geolocation and security feeds.

With Sycope you can diagnose network issues, including network connection settings and bottlenecks. The security feature of Sycope is designed based on the MITRE ATT&CK methodology. Rules and security incident detection mechanisms make it possible to detect attacks and undesirable activities on the network.

- **Visibility** – The Visibility module provides full insight into the operation of the IT network, thanks to which IT managers and network admins can quickly make decisions about resource allocation and actions to protect against unplanned downtime related to IT infrastructure failures.
- **Performance** – The Performance module is focused on L4-L7 monitoring, from TCP analytics to L7 app detection and application response times measurements. The module allows for quick triage of potential issues.
- **Security** – The Security feature allows users to detect and analyse security anomalies and threats in the context of the entire organisation. It provides support in processes such as Network Forensics, incidents and threats detection. All of this is based on the MITRE ATT@CK framework to allow security teams to easily understand detected events.