sycope

Under control now and tomorrow

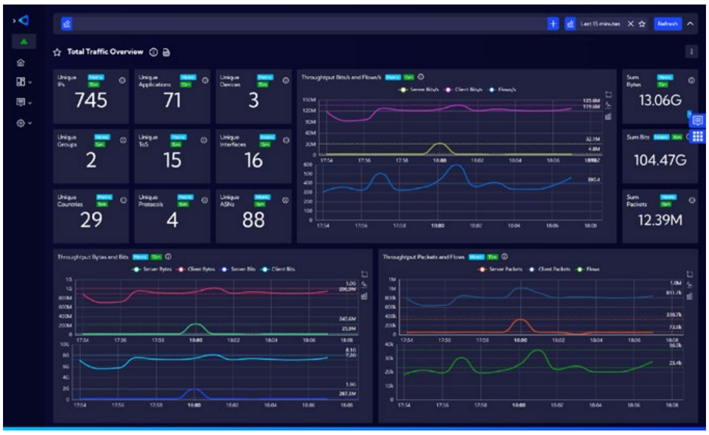
www.sycope.com

sycope

Sycope is a network performance 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.



Total Traffic Overview

Unique IPs 745

Unique Applications 71

Unique Devices 3

Unique Groups 2

Unique ToS 15

Unique Interfaces 16

Unique Countries 29

Unique Protocols 4

Unique ASNs 88

Sum Bytes 13.06G

Sum Bits 104.47G

Sum Packets 12.39M

Traffic distribution in relation to key network perspectives.

One common solution to cover multiple IT infrastructure areas

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.

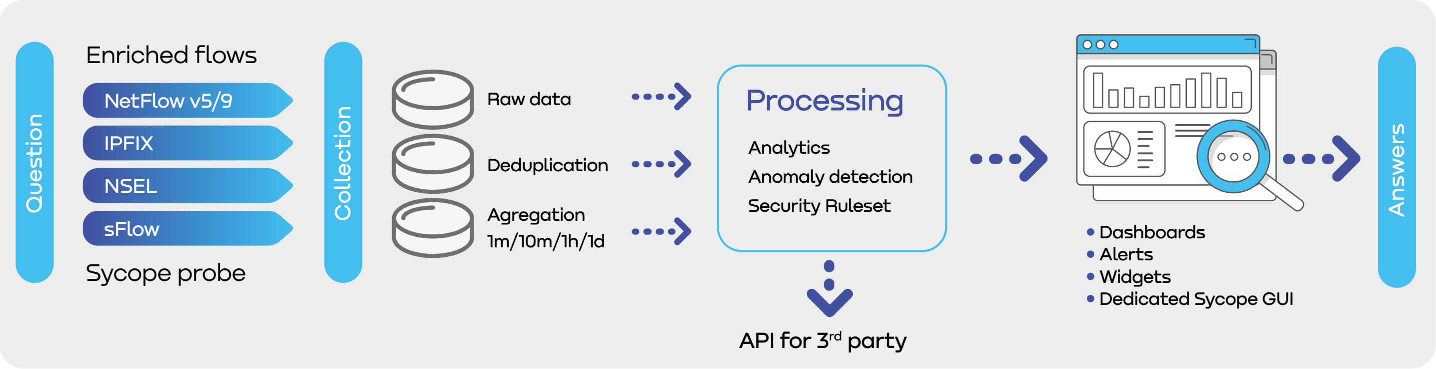
Performance

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.

We give you answers not data



Question

Enriched flows

- NetFlow v5/9
- IPFIX
- NSEL
- sFlow

Sycope probe

Collection

- Raw data
- Deduplication
- Agregation 1m/10m/1h/1d

Processing

- Analytics
- Anomaly detection
- Security Ruleset

API for 3rd party

- Dashboards
- Alerts
- Widgets
- Dedicated Sycope GUI

Answers

> “A system which is ready to work in one day - that’s not standard fare. We were pleasantly surprised at the ease of installation and integration of Sycope with our other systems”
>
> Artur Wójcik
> The biggest Oncology Center
> in Central-Eastern Europe

What we do differently

Out-of-the-box operation.

Sycope offers unique customisation capabilities, but always comes with:

- Multiple dashboards for visibility, performance and security.
- Up-to-date security feeds & rulesets.
- Alerting & reporting functions.
- Support for multiple flow protocols including non-standard fields (discovery mode).

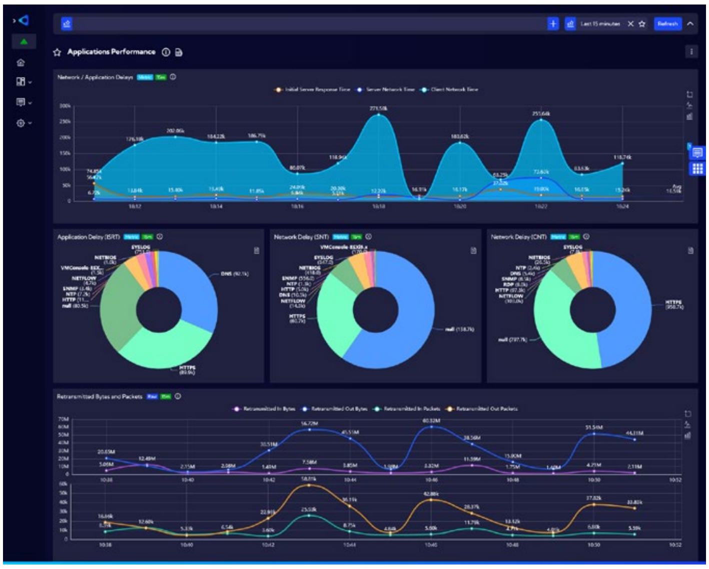
Big Data style analytics and search

Quickly filter any data, from any source, by any field, using any value and for any dashboard

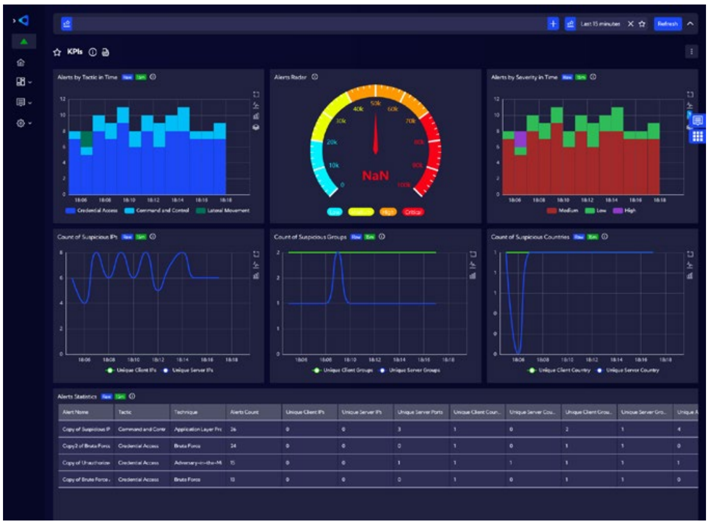
Customised dashboards and visualisation

Using the simple or advanced mode, you can create any dashboard, with exactly the same API and capabilities as the Sycope team did.

- Create your own widgets and dashboards.
- Flexible time scope for widgets.
- Private views and shared views.
- Interactive context menu and much more.



Critical metrics presentation for performance module.



Alerts Statistics

Alert Name	Tactic	Technique	Alerts Count	Unique Client IPs	Unique Server IPs	Unique Server Ports	Unique Client Coun...	Unique Server Cou...	Unique Client Grou...	Unique Server Gro...	Unique A
Copy of Suspicious IP	Command and Contr	Application Layer Pro	26	0	0	3	1	0	2	1	4
Copy2 of Brute Force	Credential Access	Brute Force	24	0	0	0	1	0	1	1	0
Copy of Unauthorize	Credential Access	Adversary-in-the-M	15	0	0	1	1	1	1	1	1
Copy of Brute Force	Credential Access	Brute Force	13	0	0	0	1	0	1	1	0

KPIs dashboards facilitate the process of monitoring trends of security risks daily.

Data deduplication

Sycope deduplicates data to always provide real and correct information, regardless of IT architecture and filters applied. Presentation of actual traffic volume values displaying the traffic path based on flow fields received for the same transmission from multiple routers.

Easy top-down access – with just a single click

The drill-down mechanisms enable you to:

- View data for a specific port, interface or IP address.

Threat detection, analysis & mitigation

Sycope consistently analyses the data to:

- Detect threats in your network and help you resolve security issues.

MITRE ATT&CK framework

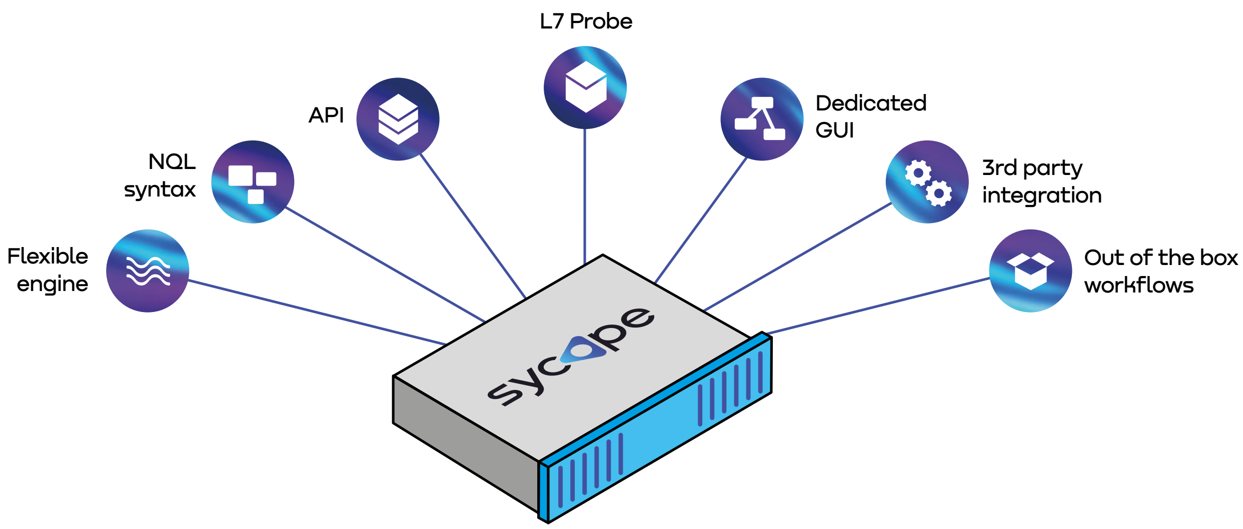
Mapping events into the MITRE ATT&CK framework

- Shows the stage of the attack.
- Describes the impact on the infrastructure.

NOC & SOC dedicated scenarios

See the big picture! All important information on a single screen to help identify the issues faster and easier.

Solution overview



Flexible engine

High performance data collection, multiple flow protocol support, embedded deduplication 2.0, discovery mode for non-standard data, allows easy development and new support for non-flow data sources.

NQL

Own query language tailored for monitoring system use cases, provides high performance for obtaining accurate data, allows for creation and calculation of any new metrics (including by the user).

API

Allows you to integrate our system with your own solutions (e.g. the Servicedesk system), as well as to create additional or custom dashboards.

3rd party integration

Utilise our API, multi-protocol notifications and embedded integration with NAC.

Out-of-the-box workflows

Selection of ready to use workflows for multiple use cases, dedicated for NOC/SOC teams, network/security forensic and business reporting.

L7 Probe

No application will remain hidden anymore. L7 app detection and application response times measurements.

sycope

Sycope is focused on designing and developing highly specialised IT solutions for monitoring and improving network performance. Our solutions were created and developed by engineers, who have been working on the issues of network performance, application efficiency and IT security, using the solutions from global APM/ NPM and SIEM providers, they have completed more than 400 projects.

www.sycope.com
contact@sycope.com

Warsaw, Poland
Goraszewska 19
02-910 Warsaw

Prague, Czech Republic
Freyova 12/1
190 00 Praha