sycope

Network performance
monitoring and security

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 bottle-necks. 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.

Application details: Critical metrics presentation for performance module.

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 down-time related to IT infrastructure failures.
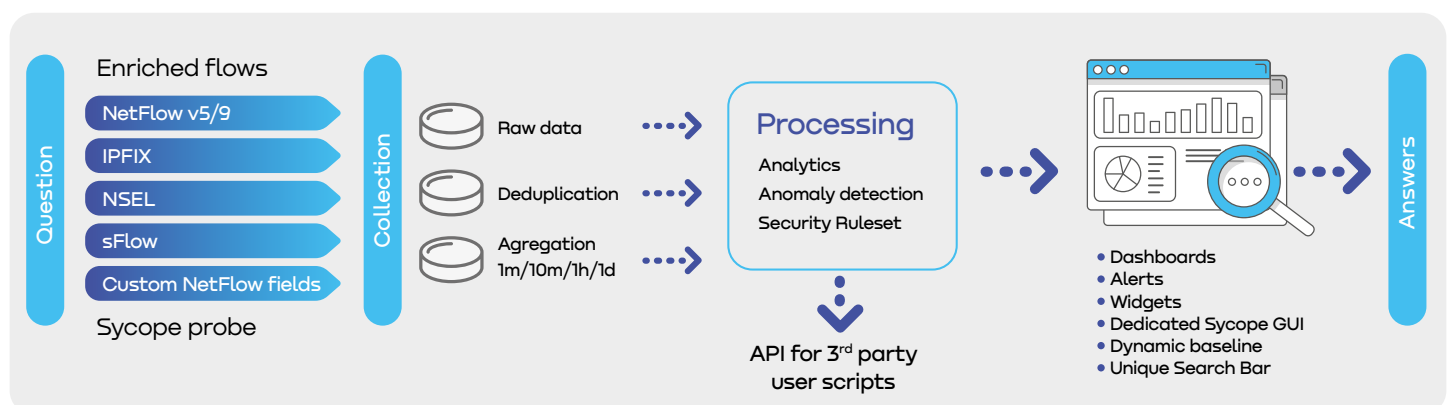
Performance

The Performance module is fo-cused 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

Enriched flows
- NetFlow v5/9
- IPFIX
- NSEL
- sFlow
- Custom NetFlow fields

Sycope probe

Question

Collection

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

Processing
Analytics
Anomaly detection
Security Ruleset

API for 3rd party user scripts

- Dashboards
- Alerts
- Widgets
- Dedicated Sycope GUI
- Dynamic baseline
- Unique Search Bar

Answers

What we do differently

Traffic summary in relation to key network perspectives.

Data minig and analytics

Dedicated, purpose-built database that is specifically designed to support the efficient storage, analysis, and retrieval of large amounts of network traffic data. This database is optimized for data mining and analytics, allowing users to easily extract insights and trends from the data collected by the system.

Powerful GUI

Sycope's GUI enhances user experience by providing easy access to data. Find information easily thanks to unique searchbar, informative visualization and customisable dashboards.
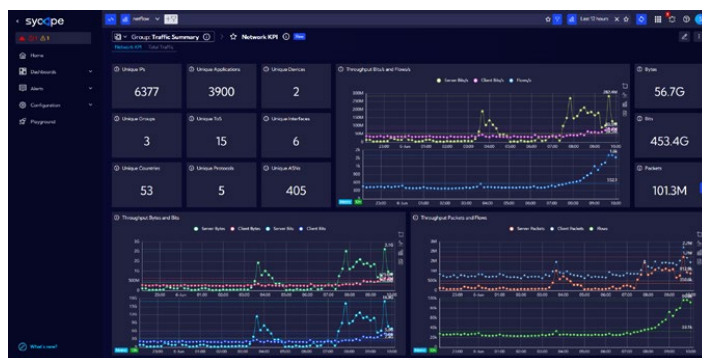
Contextual search bar simple and advanced

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

Data deduplication

Sycope remove duplicated flows from multiple sources, allowing for more accurate presentation of traffic volume and display of traffic paths based on NetFlow data. This can help organizations better understand their network usage and performance and make informed decisions about optimizing their network from multiple routers.

Extensive drill-down capabilities

The drill-down mechanisms enable you to:

- view data for a specific port, interface or IP address,
- drill-down widget, filtering widget.

Whether you're using the search bar, the stats flyout, or directly interacting with a widget or dashboard.

Threat detection, analysis & mitigation

The security module features over 60 rules covering MITRE tactics and including network threat hunting searchers. Sycope consistently analyses the data to detect threats in your network and help you resolve security issues.

Scenario based problem solving

The modules features pre-configured analytical scenarios to simplify the analysis and conclusion-making process for critical security issues.
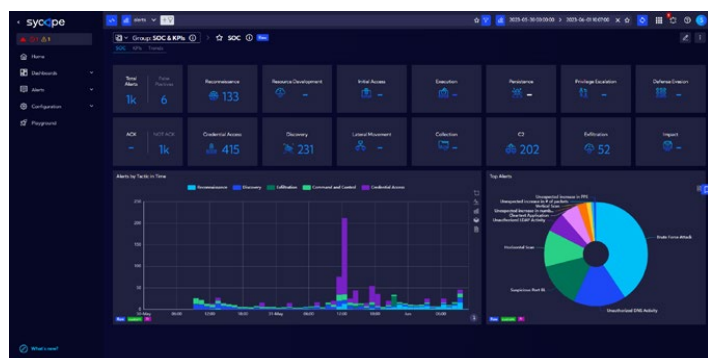
SOC & KPIS dedicated scenarios

See the big picture! All important information on a single screen to help identify the issues faster and easier.
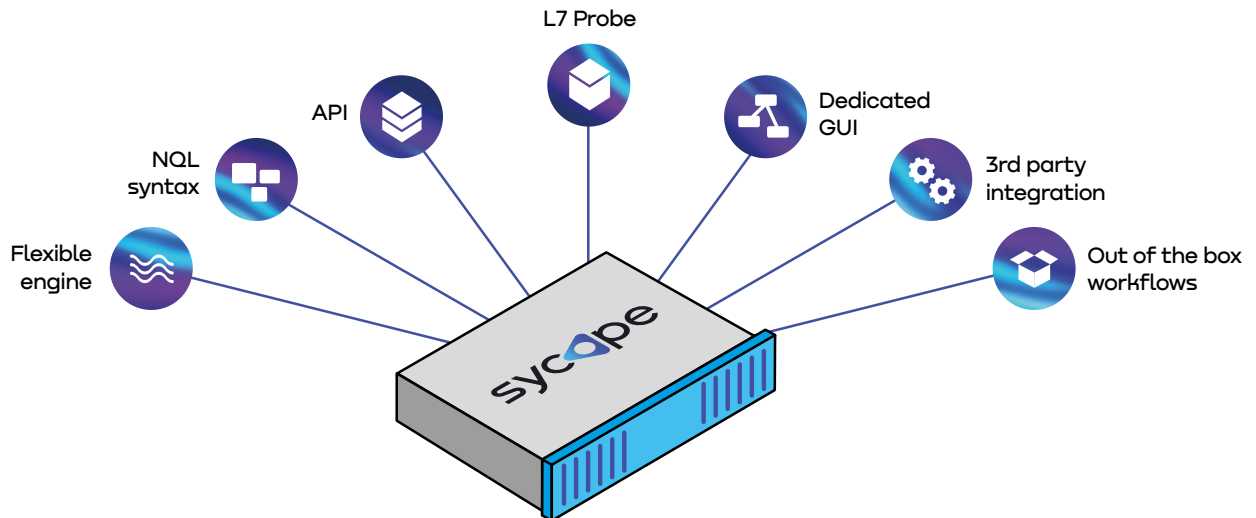
Out of the box DNS and HTTP performance metrics

Thanks to this functionality, user is able to detect trends and errors in the performance.

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

Solution overview

Flexible engine

High performance data collection, multiple flow protocol support, embedded deduplication 2.0, customised dashboards and visualization.

Discovery mode

Ability to detect and interpret new and unknown fields in the NetFlow/IPFIX/sFlow stream System remain effective and accurate, even as the data streams it processes evolve and change over time.

User scripts

Enable seamless and flexible integration with external systems or services, can be used to integrate the Sycope alerting module with these systems, allowing for data exchange, enrichment, or triggering of actions in external applications.

L7 Probe

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

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**.

Dedicated GUI

Making your work simple. Unique searchbar with search history, hinting and query builder, informative visualizations, dynamic baseline, possibility to share the views with other users.