sycope

Move security to the higher level

Sycope and macmon NAC integration

www.sycope.com

What is Sycope

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.

What is macmon NAC

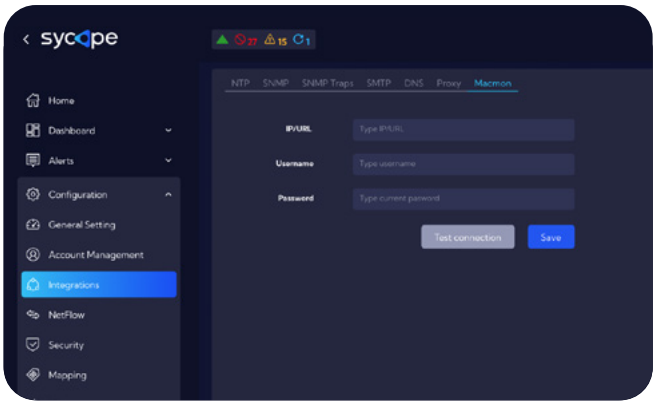
Since 2003, macmon secure has been offering infrastructure manufacturer agnostic solutions that protect heterogeneous networks from unauthorized access thanks to instant network visibility. macmon NAC is implemented quickly and easily, with significant added value for network security.
macmon NAC is a user-friendly tool that provides numerous features such as Advanced Security, Compliance, 802.1X, Guest Service, VLAN Manager, Topology, Switch Viewer, Past Viewer and more.
More information: www.macmon.eu

When one plus one is greater than two

In the world where the IT environment gets more complicated every day and new security threats attack the environment. Sycope and macmon engineers has cooperated together, to deliver the overarching security functionality. Sycope provides a very complex mechanism to analyse network traffic and detect violations of security rules. System is a 100% passive, what indicates that it does not affect the network traffic and network devices. As a consequense of that, response time to the incident is longer than for active systems, considering changes to block unwanted traffic need to be done manually by the administrator. To improve the situation and reduce response time, the administrator can integrate Sycope with macmon to detect and actively manage violation of security rules. Integration of those two systems focus on increasing value to all users.

Easy integration

Sycope is using macmon's API to send the mitigation task for a suspicious IP. All the necessary code is implemented. The only action required is to set up the credentials to the macmon system. No additional lines of code are necessary. It is as simple as that.

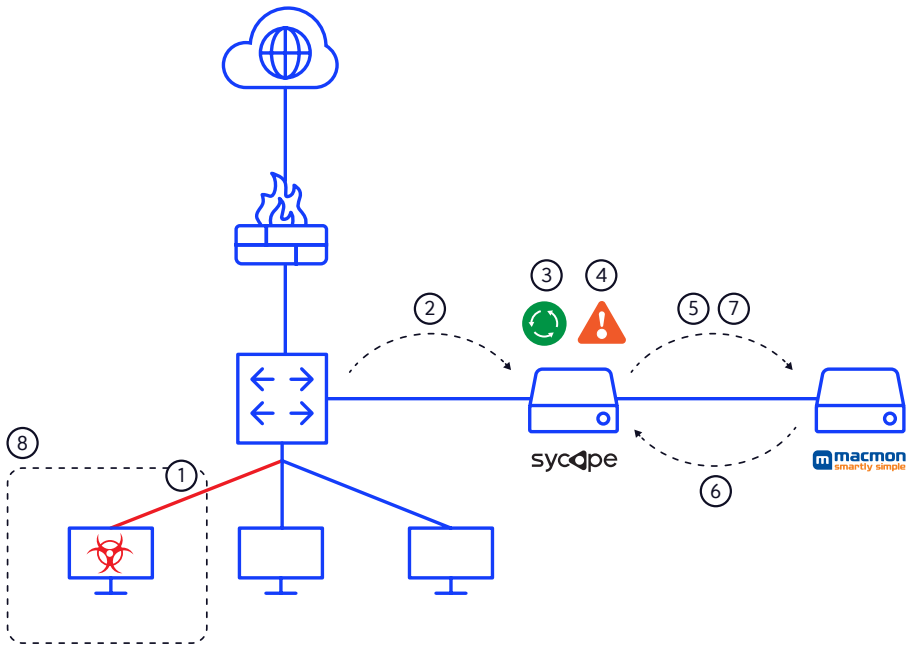


How does it work?

Every communication between hosts generates traffic in the network. Network devices use NetFlow to send information about the traffic for example communication sides, protocols and traffic volume. Sycope as a collector of NetFlow saves and analyses the information about the traffic and finds the patterns which might inform the Administrator about the security incidents and unwanted traffic. In this part, the monitoring is passive.

Integration with macmon NAC allows monitoring to be transformed into active system, blocking the unwanted traffic without manual actions. When the Alert is generated by Sycope, one of the available options is *Mitigation in macmon* . In this situation, Sycope communicates with macmon to get more information about the suspicious IP, and in the end sends the task to isolate the host. The isolating process moves the suspicious host to a separate VLAN with limited access to the internal network and Internet. Thanks to this procedure, the administrator gains time to analyse the situation and provide a remediation process.

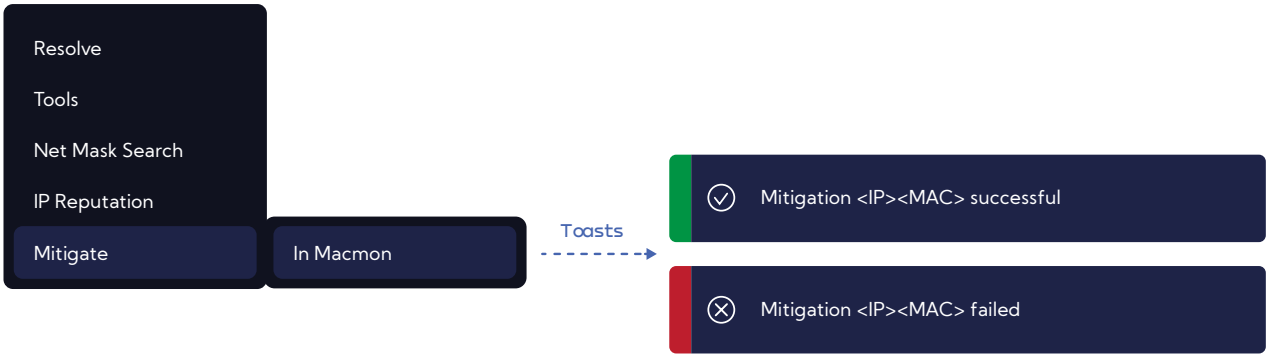
Operation diagram



1. Computer generates suspicious traffic
2. Network devices send NetFlow to Sycope
3. Sycope collects and analyses the data
4. Sycope detects suspicious traffic and generates an alert
5. Sycope sends the query about the suspicious IP to macmon
6. macmon replies to Sycope and sends the MAC Address for the suspicious host
7. Sycope sends the request to isolate the suspicious computer
8. macmon communicates with the network device and sends the request to move the computer to the isolated network

Additional ways to block unwanted IPs

There are two ways to block unwanted IPs. The first one is automated (explained in the schema diagram). When the Alert is triggered, you can select the mitigation action in the rule and send the task to block the IP. The second one is manual. You can right-click on every internal IP address and select *Mitigation in macmon*.



Integration between Sycope and macmon converts the passive monitoring system into the NDR (Network Detect and Response) system. This approach helps protect the network and moves security to a higher level.

About Sycope

Sycope was 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 National Defence, NATO, National Bank of Poland, T-Mobile, Ikea, ING Group, Orange and Alior Bank. 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 Sycope was created.

Contact us:
Sycope
Goraszewska 19,
02-910 Warsaw, Poland
contact@sycope.com

About macmon

macmon secure develops network security software, focusing on Zero Trust Network Access for Networks and Clouds. Founded in 2003, macmon secure has grown from strength to strength, becoming the technology leader in the field of Network Access Control. Based in Berlin, the macmon NAC solution is fully engineered in Germany. The products macmon NAC (Network Access Control solution) and macmon SDP (Secure Defined Perimeter) are used worldwide to protect networks and cloud resources from unauthorised access.

Contact us:
macmon secure GmbH
Alte Jakobstrasse 79-80
10179 Berlin, Germany
info@macmon.eu