sycope

CASE STUDY

Sat Film Sp. z o.o.

Description of the application of an IT network monitoring solution based on network flows – Sycope

Recipient
Sat Film Sp. z o.o.

Requirements
Implementation of a tool for network traffic analysis and threat detection, especially DDoS attacks. Enabling rapid deployment of the system and real protection against threats.

Solution
Sycope

Implementation partner
Passus S.A

Conditions

Sat Film is a Polish network and cable TV operator. The company has its headquarters in Włocławek and Łódź. It offers digital television, fixed and mobile telephony services and broadband Internet access. It is the 8th largest cable operator in Poland in terms of number of subscribers. It provides access to 160 channels on its own digital platform, including over 120 channels in HD quality. It delivers Internet services based on DOCSIS, GPON, Wi-Fi and mobile technologies, offering several different bandwidth packages. The company is a local ISP, responsible for creating connections on a regional scale; its core tasks include providing customers with stable Internet access, redirecting Internet traffic, and maintaining the technological infrastructure. The company has an extensive technical department to support network continuity. From the customer's perspective, it is very important to defend against all types of threats that can negatively affect the telecommunications network and access to services by its users. In such a situation, network monitoring has become a key objective in order to quickly locate attacks and neutralize them.

The telecommunications industry in which the client operates is facing an increasing trend of all kinds of cyber attacks. In Q1 2021, the most common form were DDoS attacks. An additional factor in the rise of cybercrime may be the decreasing cost of tools for launching cyber attacks. For just a few euros, access can be purchased to a so-called botnet, allowing a volumetric DDoS (Distributed Denial of Service) attack to be carried out.

The client's situation

One of the biggest problems the client has faced as a local Internet operator are DDoS attacks, which have led to clogged lines, lack of Internet access and, above all, an impact on dissatisfied customers who, in extreme cases, may have decided to terminate their subscriber contracts due to the lack of signal. This has had a negative impact on business. The specific nature of DDoS attacks requires constant monitoring as they cannot be predicted. Initiating network monitoring with a protocol like NetFlow would help prevent the significant consequences and costs resulting from even a small attack. This is especially true in the case of local ISP operators who, due to the scale of their operations, have much smaller budgets than the largest players on the market.

A small operator with only a few thousand terminals experiences serious repercussions from any attack carried out on its network. Unfortunately, the attack is not only felt by the attacker, but by all customers of the operator concerned. A clogged edge router, which is at the interface between the network and the Internet, will cause problems for all network users. One of the customer's main criteria when looking for a network monitoring solution was a solution that would allow them to monitor network traffic collected from the edge router, offering the ability to quickly detect performance problems and security incidents and anomalies. The challenge was to find a high-performance, cost-effective monitoring tool which would allow for analysis of all network traffic, both in terms of performance and security.

Course of works

Given the critical nature of having a network monitoring tool with a focus on DDoS attacks, the client decided to purchase and implement Sycope's solution based on NetFlow-type protocol analysis. The decision to purchase was preceded by prior testing of the tool by the company's internal IT department. The system was ultimately not integrated with other tools. The solution was implemented in October 2020; the implementation and launch of Sycope itself took one day. The team appreciated the quick and efficient installation of the system. With local support and an intuitive interface, the entire internal IT department was able to move to full use of all modules from day one.

Solutions and benefits

The Sycope system enabled the client to analyze network traffic using a NetFlow-like protocol, including the mitigation and identification of both single and multi-vector DDoS attacks of varying intensity. Sat Film began collecting and analyzing data from network flows, diagnosing causes with network connections and detecting DDoS attacks of varying intensity.

Currently, the Sycope system for the IT department functions as the sole and most important tool for analyzing network traffic, including DDoS attacks. The client mainly focuses on detecting volumetric attacks that reduce the availability of a service by saturating a network connection, as well as on attacks on a protocol that exploit a specific property or vulnerability in a given protocol. Through these measures, it ensures that its customers have uninterrupted access to the service, positively influencing their satisfaction with their choice.

The customer's IT department paid particular attention to the ability to flexibly set rules to detect attacks. When monitoring flows, the customer has the option of using both static and dynamic parameters. Static parameters allow the values used in the attack identification process to be defined, e.g. the number of source IP addresses, bytes, flows. Dynamic parameters make it possible to determine permissible deviations from the so-called baseline, which is created based on a comparison of current and historic traffic characteristics.

Predefined dashboards for multidimensional analysis of attacks facilitate daily work with the tool at the customer's premises. At Sat Film, these dashboards are used to determine the start and end time of an attack in the context of the service under attack and the group to which the host belongs, or to determine the type of service under attack. This responds to the customer's need for information – who is attacking whom – and also enables advanced analysis.

In the coming months, the client's IT team plans to launch automatic attack mitigation after additional testing with manual IP blocking to protect the system from unwanted traffic.

"A useful tool that allows you to easily monitor network performance and respond to events that occur."
Marek Barański, Sat Film network administrator

sycope

www.sycope.com

Get In Touch

Warsaw, Poland
Goraszewska 19
02-910 Warsaw

Prague, Czech Republic
Freyova 12/1
190 00 Praha

contact@sycope.com