NTA has now become NDR.

Obtaining visibility and deep insight into network traffic is something many organizations should focus on. The majority of all cyber-attacks leave a trail in network traffic. The network contains valuable information about threats here and now, as well as vulnerabilities. And as they say,

Packets Don't Lie.

However, the large amount of data that goes through the network makes it easier for hackers to hide their tracks and avoid being detected. When hackers interfere with normal traffic in the network, it will make it easier for them to hide and fulfill their work without being detected.

Given the volume of threats and the increase of more sophisticated attacks, current signature-based detection solutions cannot keep up. Detection of known indicators is no longer sufficient. Organizations need solutions that can help create a baseline and detect abnormal behavior in the network before it is too late.

It is about gaining insight into the network and having enough context to make quick decisions. It is required to create deep visibility in network data, to achieve a meaningful context for its analysis. This visibility must, of course, be so close to "real-time" that the IT expert can react here and now.

Any organization that wants to improve its overall security should look into NDR as a central part of its IT security strategy.

What is NDR?

It stands for network detection and Response. It comes from NTA (Network Traffic Analysis). But... In 2020, the terminology was changed to NDR.

NDR platforms analyse the behavior of network traffic using non-signature-based techniques (advanced), which also include various methods of machine learning, artificial intelligence, and of course security specialists.

In addition to north/south traffic, it also looks at east/west traffic. You create a baseline of your traffic and can then detect abnormalities in the traffic.

The **response part itself** can be either manual or automatic, which has advantages/disadvantages. You can only automate what you are sure of, and there is still big uncertainty in cyber security.

It is easy to shut down an endpoint with EDR without human interaction. Typically, isolating the hosts and remediating it, someone just buys a new one. But the network is too large and complex to automatically shut down all things.

Gartner's requirements for an NDR platform are as follows:

· *Analyze raw network packet traffic or traffic flows (for example, NetFlow records) in real time or near real time.*

· *Monitor and analyze north/south traffic (as it crosses the perimeter), as well as east/west traffic (as it moves laterally throughout the network).*

· *Be able to model normal network traffic and highlight suspicious traffic that falls outside the normal range*

· *Offer behavioral techniques (non-signature-based detection), such as machine learning or advanced analytics that detect network anomalies.*

· *Provide automatic or manual response capabilities to react to the detection of suspicious network traffic.*

What are the benefits / benefits of NDR?

· You can quickly and efficiently detect suspicious patterns in encrypted traffic.

· Identify abnormal traffic behaviors, such as call-home activity from third-party vendors, making it easier to maintain data security.

· There are several environments where you can not install endpoint detection (EDR), such as IoT, OT, and ICS. NDR is an ideal solution to create this visibility and stop potential attacks, thus removing blind spots.

· Reduce the number of false positives and free up resources to focus on specific threats here and now.

· Discover “Insider threats” such as shadow IT and misconfigurations. You will also identify which assets there are at the network.

· NDR complementary a SOC, (Gartner SOC Visibility triad). It is necessary for a well-functioning SOC today.

Conclusion: With NDRyou will detect threats that are not known at an early stage in your network. This reduces the risk of being compromised, which has the effect of saving time and money.