SECUINFRA
Cyber Defense. Made in Germany.

Professional article

Network-based security approach: Network Detection & Response (NDR) as part of the cyber defense strategy

With the network-based security approach Network Detection and Response (NDR), the entire data traffic of a company can be continuously monitored and analyzed - based on static rules, machine learning and threat intelligence. The solution includes all internal data traffic as well as external communication, thus taking into account sources such as client and server systems, network components, but also IoT sensors or OT devices. The thus achieved deep understanding of normal network behavior leads to a reliable and fast identification of anomalies.

The 6 most important features of NDR are:

- Network traffic monitoring: an NDR solution monitors and analyzes network traffic for potential threats. This can be done by using technologies such as intrusion detection systems (IDS) and intrusion prevention systems (IPS).
- Behavioral analysis: an NDR solution uses machine learning algorithms to analyze the behavioral pattern of network traffic and detect anomalies that may indicate a potential threat.
- Automatic response: an NDR solution can automatically respond to detected threats by, for example, disconnecting network connections or implementing rules in the firewall system.
- Integrity protection: An NDR solution can also ensure that the integrity of the network is maintained by monitoring changes to configurations and by monitoring unauthorized access to network resources.
- Reporting and forensics: An NDR solution provides the ability to generate detailed reports and forensics data that can help investigate security incidents and identify attackers.

However, to realize effective, sustainable and reliable threat detection, NDR needs to work in tandem with other solutions.

Detect and respond to network threats

By systematically and automatically monitoring traffic and network behavior, NDR solutions learn "normal behavior." If patterns deviating from this learned behavior occur, such as suspicious access to systems or data exfiltration, the NDR solution automatically triggers an alert.

Ideally, the alerts should be collected centrally, for example in a security information and event management (SIEM) system, and correlated with other data, for example from an endpoint detection and response (EDR) solution. With the help of the SIEM, the cyber defense analyst can analyze irregularities that occur centrally and efficiently and, if necessary, respond to them in a targeted manner. The support of a SOAR system (Security Orchestration Automation and Response) is advantageous here.

The result of the interaction of these detection and response solutions is a significantly improved level of IT security for companies, through which it can be achieved that even sophisticated cyber attacks can be identified and defended against at an early stage.

Here's how NDR can support SIEM

Both NDR and SIEM collect and share information and work together on that basis with the overarching goal of detecting, verifying and responding to threats.

Once an attack is identified, an NDR solution can automatically respond by isolating affected devices to prevent the spread of the attack and clean up affected areas. Furthermore, the NDR solution makes all collected information available to the SIEM system.

Specifically, NDR supports the SIEM by:

- Collecting and analyzing connection data from network traffic.
- Providing an immutable data source
- Optimizing complete, comprehensive reports
- Covering log gaps
- Log analysis as well as aggregation and detection of behavioral threats.

The SIEM uses this information, along with other events from various security devices and applications in real time, and correlates this data to detect potential threats and generate alerts. Cyber defense analysts also use the information gathered by NDR to, in turn, adjust detection rules in the SIEM to better detect and defend against future attacks.

Complementing NDR with EDR

The focus of Endpoint Detection & Response (EDR) solutions is to increase the visibility of anomalies at the endpoint: protection occurs directly on endpoints, not at the network perimeter. Endpoints - any device connected to a network - are potential gateways for cyber threats. With EDR, endpoint activity is captured, logged and analyzed in real time. As such, EDR solutions are a valuable part of the cyber defense toolset, but their focus on endpoints means they are not able to monitor network traffic and activity that occurs outside of the endpoint. This type of monitoring and analysis requires a Network Detection and Response (NDR) solution. As a result, the technologies complement each other ideally, resulting in a more detailed security picture through the correlation of the information gathered and the ability to comprehensively detect and defend against attacks.

Conclusion

SOC teams still rely heavily on endpoint detection and response (EDR) and security information and event management (SIEM) tools in their work. However, these tools cannot provide visibility into traffic and thus only provide a small, very limited slice of security-related activity. Only when supplemented with an NDR can cyberattacks be detected, analyzed, and targeted at an early stage. The combination of NDR, EDR and SIEM makes it possible to detect threats and attacks at the application, network and endpoint level and to react immediately.

Authors: Ramon Weil - Founder & CEO - SECUINFRA GmbH

Norbert Nitsche - Head of Cyber Detection & Response Center - SECUINFRA GmbH

Further information: https://www.secuinfra.com/de/techtalk/die-rolle-von-network-detection-response-bei-der-effektiven-bedrohungserkennung/

Contact: SECUINFRA GmbH
Svenja Koch
Stefan-Heym-Platz 1
10367 Berlin
Deutschland

Tel. +49 (0) 160 921 633 44
svenja.koch@secuinfra.com