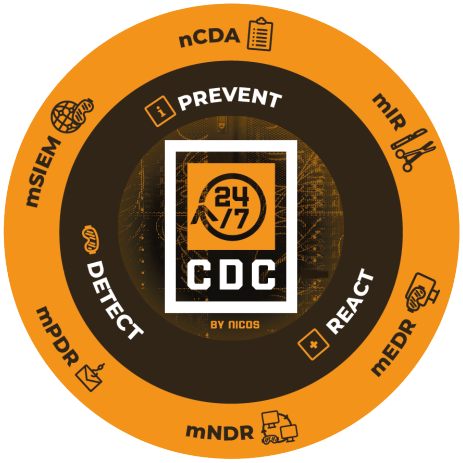
nicos cyber defense
xantaro group

nicos MANAGED DETECTION & RESPONSE SERVICES



WE PROTECT YOUR COMPANY FROM CYBER ATTACKS

The **24/7 nicos CYBER DEFENSE CENTER (nCDC)** is the basis for processing alarms of all kinds - around the clock, 365 days a year. This process is standardized based on individual agreements in so-called runbooks, which precisely describe the procedure. Best-practice automations are also used to respond quickly, in a coordinated and reproducible manner in urgent cases requiring immediate action. Scaling matrices and other documents agreed upon with the customer ensure a rapid, collaborative response in critical situations.

nicos MANAGED SECURITY SERVICES: CAN BE BOOKED ON A MODULAR BASIS

nicos mNDR (mIDS/mIPS) - Managed NETWORK DETECTION & RESPONSE

With our mNDR Service including **M**anaged **I**NTRUSION **D**ETECTION **S**YSTEM (mIDS) and **M**anaged **I**NTRUSION **P**REVENTION **S**YSTEM (mIPS), we receive the alarms from the main components of network security (e.g. IDS/IPS systems or proxy systems) and forward them to the 24/7 nicos CYBER DEFENSE CENTER for processing. The focus here is on IDS/IPS alarms. Command-and-control or botnet communications are particularly relevant in identifying devices controlled by attackers at an early stage and remediating them immediately.

nicos mPDR - Managed PHISHING DETECTION & RESPONSE

Emails are still the main gateway for cyber criminals. With the nicos mPDR service, we evaluate emails flagged as suspicious in a secure environment. With the knowledge gained, similar emails can be deleted from mailboxes and optimizerd using email filters.

nicos mEDR - Managed ENDPOINT DETECTION & RESPONSE

We receive the alarms from the customer's own EDR system via the nicos mEDR service. The alarms are processed in the 24/7 nicos CYBER DEFENSE CENTER. The nicos mEDR service enables analyses and reactions directly on the devices via live response. This enables us to obtain forensic artefacts, analyze processes and initiate targeted responses in a timely manner. We prefer the EDR systems Microsoft Defender for Endpoint, Crowdstrike and SentinelOne.

nicos mSIEM - Managed SECURITY INFORMATION & EVENT MANAGEMENT

By using a SIEM system, we establish comprehensive real-time monitoring of the customer's IT infrastructure with regard to typical behaviour-based approaches of attackers. nicos mSIEM offers the possibility to formulate and create highly individual use cases and detection rules. In addition, a SIEM also serves as an analysis and reporting tool - especially in the case of major security incidents, it is helpful to review the infrastructure over the past few months.

nicos mIR – Managed INCIDENT RESPONSE

With the nicos mIR service, we are ready for emergencies 24/7. This service is used for ad-hoc response to cyber attacks and is part of a holistic protection against cyber attacks. nicos mIR is based on seamless monitoring of cyber threat indicators by the 24/7 nicos CYBER DEFENSE CENTER.

YOUR PARTNER FOR CYBER ATTACK ANALYSIS AND DEFENSE.

Julian Reiber
Sales Engineer

E jreiber@nicos-cdc.com
T +49 251 986 33-5624

Lukas Richter
Sales Engineer

E lrichter@nicos-cdc.com
T +49 251 986 33-5621

www.nicos-cdc.com