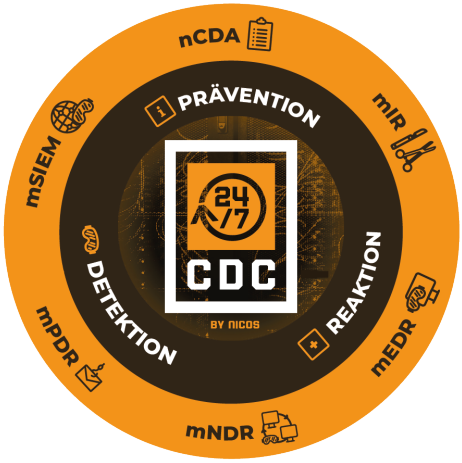
nicos cyber defense
xantaro group

nicos MANAGED DETECTION & RESPONSE SERVICES



WIR SCHÜTZEN IHR UNTERNEHMEN VOR CYBERANGRIFFEN

Das **24/7 nicos CYBER DEFENSE CENTER (nCDC)** ist die Grundlage für die Bearbeitung von Alarmen jeglicher Art - rund um die Uhr, an 365 Tagen im Jahr. Dies geschieht standardisiert, auf Basis individueller Absprachen in sogenannten Runbooks, die die Vorgehensweise exakt beschreiben. Hierzu werden auch Best-Practice-Automationen eingesetzt, um in dringenden Fällen mit unmittelbarem Handlungsbedarf schnell, abgestimmt und reproduzierbar zu reagieren. Eskalationsmatrixen und weitere, in Abstimmung mit dem Kunden vereinbarte Dokumente stellen in entscheidungskritischen Situationen die schnelle, gemeinschaftliche Reaktion sicher.

nicos MANAGED SECURITY SERVICES: BEDARFSGERECHT & MODULAR BUCHBAR

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

Bei unserem mNDR Service **M**anaged **I**NTRUSION **D**ETECTION **S**YSTEM (mIDS) und **M**anaged **I**NTRUSION **P**REVENTION **S**YSTEM (mIPS) erhalten wir die Alarme aus den wesentlichen Komponenten der Netzwerksicherheit (z.B. IDS/IPS Systeme oder Proxy Systeme) und leiten diese zur Bearbeitung an das 24/7 nicos CYBER DEFENSE CENTER. Dabei stehen die IDS/IPS Alarme im Vordergrund. Insbesondere Command-and-Control oder Botnet-Kommunikationen sind relevant, um durch Angreifer kontrollierte Geräte frühzeitig zu identifizieren und unverzüglich zu bereinigen.

nicos mPDR - Managed PHISHING DETECTION & RESPONSE

E-Mails sind noch immer Haupteinfallstore für Cyber-Kriminelle. Mit dem nicos mPDR Service bewerten wir die als verdächtig deklarierten E-Mails in gesicherter Umgebung. Mit den gewonnenen Erkenntnissen können gleichartige E-Mails in Postfächern gelöscht und per E-Mail-Filter optimiert werden.

nicos mEDR - Managed ENDPOINT DETECTION & RESPONSE

Über den nicos mEDR Service erhalten wir die Alarme des kundeneigenen EDR-Systems. Die Alarmverarbeitung erfolgt im 24/7 nicos CYBER DEFENSE CENTER. Der nicos mEDR Service ermöglicht Analysen und Reaktionen direkt auf den Geräten per Live Response. So ist es uns möglich, forensische Artefakte zu beschaffen, Prozesse zu analysieren und zielgerichtete Reaktionen zeitnah einzuleiten. Wir präferieren die EDR-Systeme Microsoft Defender for Endpoint und SentinelOne.

nicos mSIEM - Managed SECURITY INFORMATION & EVENT MANAGEMENT

Durch den Einsatz eines SIEM-Systems etablieren wir ein flächendeckendes Echtzeitmonitoring der Kunden-IT-Infrastruktur bezüglich typischer verhaltensbasierter Vorgehensweisen von Angreifern. nicos mSIEM bietet die Möglichkeit, hochgradig individuelle Use Cases und Detection Rules zu formulieren und zu erstellen. Zusätzlich dient ein SIEM auch als Analyse- und Berichtswerkzeug – insbesondere bei größeren Sicherheitsvorfällen sind Betrachtungen der Infrastruktur über die vergangenen Monate hilfreich.

nicos mIR – Managed INCIDENT RESPONSE

Mit dem nicos mIR Service sind wir 24/7 einsatzbereit für den Ernstfall. Dieser Service dient der Ad-hoc-Reaktion auf Cyber-Angriffe und ist Bestandteil eines gesamtheitlichen Schutzes vor Cyber-Attacken. nicos mIR basiert auf einer nahtlosen Überwachung von Cyber Threat Indikatoren durch das 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