# **Operation Center (SOC) Services**

NETDESCRIBE | XANTARO | NICOS



#### **Network Detection &** Response

- Analyse der IDS/IPS Alarme
- Überwachung der Netzwerk-Kommunikation



#### **Endpoint Detection** & Response

- Analyse der EDR-Alarme
- Reaktionen direkt auf den Endgeräten



#### Incident Response

- 24/7 einsetzbereit für die Reaktion im Ernstfall
- Ad-Hoc Reaktion, Krisenmanagement, **Forensik**



#### **Cyber Defense Assessment**

- Überblick über das Sicherheitsniveau
- Priorisierte Empfehlungen zur Verbesserung



# Simulation

realistischer Angriffe





#### **Phishing Detection** & Response

• Bewertung verdächtiger **Emails** 



#### mSIEM/mXDR

- Flächendeckendes **Echtzeit-Monitoring**
- Korrelation verschiedener Sensoren
- Individuelle UseCases und Detections



#### **Secure Access** Service Edge

- Netzwerklösungen mit "Fnde-zu-Fnde" Sicherheit
- Sicherheitsabdeckung für das globale Netzwerk



### **Pentesting**

- Technische Sicherheitsüberprüfung
- Evaluation von Schwachstellen



MNDR



• Sicherheitssysteme auf die Probe stellen durch simulation

# Red, Blue & Purple Teaming

MPDR

- Angreifer und Verteidiger optimieren sich gegenseitig
- Simulation von Angriffen und Test der Reaktionsmittel, -wege und Prozesse sowie Wiederherstellung

### Warum Xantaro Group (NetDescribe | Xantaro | nicos)?

Die Xantaro Group ist ein international führender Solution Provider in den Bereichen High-Performance-Netzwerke, IT-Sicherheitslösungen und Managed Services für Carrier, Service Provider und Industriekunden:

 Abdeckung der OSI-Layer 1-7 mit den besten Experten des Marktes

• Führendes Team von Netzwerk- und Security-Spezialisten mit insgesamt über 800 Zertifizierungen

Unsere Experten freuen sich darauf, mehr über Ihre Anforderungen zu erfahren!



info@xantaro.net



www.xantaro.net