Adva
NETWORK SECURITY

Data Sheet

SOC-as-a-Service

24/7 security monitoring and threat prevention as a managed service

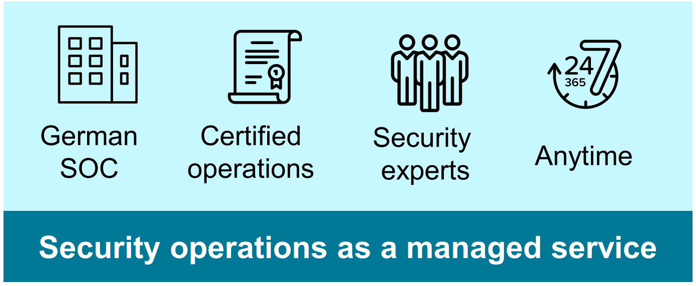
Benefits

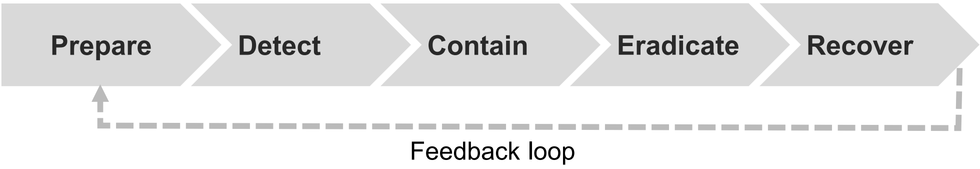
- **Minimal attack surface**
  Analysis of vulnerabilities and elimination of security gaps
- **Fast response**
  Comprehensive attack detection enables quick and effective countermeasures
- **Flexibility and efficiency**
  External resources instead of in-house security technology and personnel
- **Protection around the clock**
  24/7 monitoring through our SOC based in Germany
- **Comprehensive expertise**
  Experienced security experts and proven, AI-supported processes
- **Regulatory compliance**
  Legal compliance with both existing and new regulations

Overview

The increasing threat of cyberattacks calls for efficient measures to quickly detect and respond to security incidents. These tasks often overwhelm IT security teams. A security operations center (SOC) as a managed service offers a cost-effective way to protect companies with high security requirements from the negative consequences of cyberattacks.

We provide our customers with a customized combination of SOC components tailored to their specific needs. Our security solutions include vulnerability and attack detection as well as threat analysis. All information is centralized in our central control center, where our SOC experts evaluate it. They develop effective threat defense strategies and coordinate them with the customer. The managed SOC-as-a-Service reliably protects companies against data loss and network disruptions, preventing production downtime and damage to their reputation. It also complies with NIS-2 and other cybersecurity regulations.





Technical components

Network detection and response (NDR)

Our 24/7 network monitoring service reliably detects attacks by evaluating messages from network elements and their login data. This enables the identification and isolation of unwanted data traffic, stopping malware infiltration immediately. NDR not only identifies known attack vectors but also detects zero-day attacks by recognizing atypical traffic patterns.

Endpoint detection and response (EDR)

Threat prevention in the end device is crucial as compromised devices are often the starting point for serious attacks. EDR prevents malware infiltration of malware and the unauthorized outflow of data. It continuously monitors all processes and procedures, enabling rapid responses to security incidents. EDR also blocks connections to compromised network nodes and prevents devices from participating in botnets.

Security information and event management (SIEM)

The collection of security information and defense coordination is handled by SIEM. It gathers and correlates log data and messages from IT infrastructure components such as firewalls and intrusion detection/prevention systems. This information is used to detect anomalies and security incidents. Our SOC security experts recommend and initiate effective defensive measures and draw up recommendations for strengthening the IT infrastructure.

Vulnerability assessment system (VAS)

Identification and elimination of vulnerabilities requires to record installed hardware and software, comparing them with known vulnerabilities to identify and prioritize the right measures. Misconfigurations and inadequately protected interfaces are also identified. Penetration tests validate the results. In addition, we provide our customers with recommendations for hardening their IT systems.

Threat intelligence service (TIS)

In response to changing threat situations, protective measures must be continuously updated based on current threat information. Our knowledge of attack tools and the latest attack trends enables us to take targeted action. This analysis is based on information from state security authorities, IT security consultancies, security forums and public sources (Open Source Intelligence, OSINT). Specific measures include awareness training, password renewals, backup checks and adjustments to emergency plans.

Adva
NETWORK SECURITY

For more information please visit us at www.advasecurity.com

Product specifications are subject to change without notice or obligation.