

Security Operation Center

Detect and block threats in a timely manner



Attacks are becoming more sophisticated

Safety has become the Achilles' heel for many companies. Stability remains and success only succeeds if the protection of their own data is guaranteed. But this is becoming increasingly difficult because data saboteurs are extremely unscrupulous. Viruses are transmitted through e-mails, USB sticks or by accessing manipulated web-sites, Trojans and other malware into corporate networks and cause great damage. Via external access attackers manipulate network components in order to gain access to networked application servers. Denial of service attacks are often sufficient to paralyze entire branches of business by blocking applications.

Control and fast reaction

There's no way around it: If you want to protect your company comprehensively, you have to keep an eye on your security-relevant systems and applications. At the same time, you should be able to take immediate action in the event of an attack. For this you need the right tools and trained experts with the workfocus on IT security. Our BSI-certified Security Operation Center is modular as follows that it fits exactly to your requirements.



Defense + Prevention

In our SOC, we monitor all activities in networks with the aim of detecting anomalies immediately. We not only work with our own security platform, but also integrate your existing solutions if required. Companies that do not want to invest in complex tools and a team of experts themselves have an alternative to operating their own security operation center with us. As an MSSP (Managed Security Service Provider), we have the right expertise and the necessary experience.

Our SOC team keeps an eye on your important applications and is trained to handle even new, unknown sabotage methods quickly. If a problem cannot be directly averted, we immediately alert and support the recovery if necessary.

Our SOC tasks depend on your needs.

Here are a few examples:

- alerting in case of suspicious or predefined anomalies
- orchestrate, automate, and respond to incidents in real-time with our Security Information and Event Management (SIEM) Platform
- Next Generation End Point Security with Machine Learning
- Asset & Device Management for Network Access Control
- two-factor authentication
- component-related vulnerability analysis, from the inside and outside
- support in isolating and restoring the affected systems and networks



Certified by the BSI

The dacoso Security Operation Center has been approved by the BSI (German Federal Office for Security in Information Technology) the „ISO 27001 certificate based on basic IT protection“. This officially confirms that we „ensure information security and the successful implementation of international standards using the IT-Grundschutz methodology internally and externally“ (BSI). The BSI seal is the convincing proof of security at the highest level, not only for security-conscious companies, but also for all companies that want to protect their data reliably.



Advantages of SOC

- 24/7 operated operation
- all services on demand according to the high requirements of the BSI
- modular concept: SOC services are freely selectable
- high security container for all monitoring servers and network components
- optional SOC support in case of failure: from consulting to spare parts delivery
- SOC management from Germany, with technicians trained here
- German-language support throughout, if required also in English

Flexible price models

When you use our SOC, you benefit from OPEX advantages because you do not invest yourself. The costs will be invoiced via a monthly usage fee. Of course, the price is also regulated according to different aspects, for example:

- desired tasks and responsibilities
- number of sites to be monitored
- SLA specifications (response times, escalation times)
- minimum contract duration



The addition: Network Operation Center (NOC)

In our NOC, in particular your network connections and the hardware used are under professional control. Our NOC employees take immediate action when problems arise and restore the systems. The main tasks:

- monitor hardware and connections
- provisioning and configuring networks
- operate networks and keep them up to date
- proactively predict errors
- provisioning and configuring networks
- operate networks and keep them up to date
- proactively predict errors
- alert immediately in case of security problems
- initiate the repair at an early stage



We can integrate different platforms into the NOC and look at networks under very specific aspects. These include the network technology from ADVA Optical Networking, the carrier-grade equipment from NOKIA and the WAN Optimizer from InfoVista (Ipanema). Also the encryption solutions of atmedia, whose smooth functioning is ensured by the monitoring. The NOC is also used for virtualized networks. Especially with these relatively new network solutions the right people and the right equipment are needed to control the SD WANs. The dacoso-NOC was certified by the BSI with ISO-27001 on the basis of IT-Grundschutz.



dacoso
data communication solutions

dacoso GmbH

Deutschland | Robert-Bosch-Str. 25a | D-63225 Langen | T +49 6103 404 569 0

Schweiz | Riedstr. 1 | CH-8953 Dietikon | T +41 44 371 78 77

Österreich | Am Europlatz 2 | A-1120 Wien | T +43 1 717 28 324

info@dacoso.com | www.dacoso.com