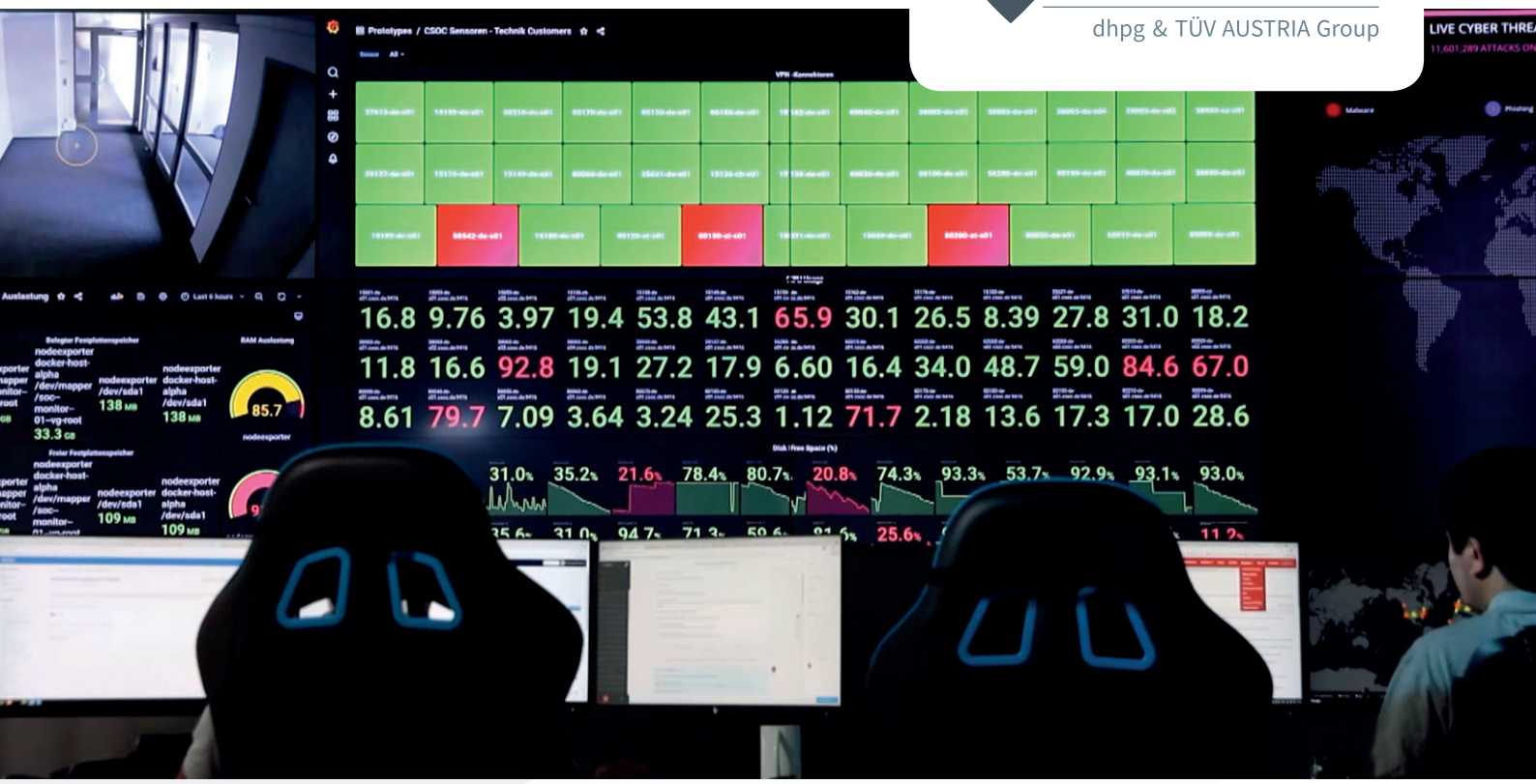
dhpg & TÜV AUSTRIA Group



CERTIFIED SECURITY OPERATIONS CENTER GmbH (CSOC)

SOC as a Service

SOCaaS – the core service of CSOC

The SOC as a Service monitors the client‘s IT systems to detect possible cyber attacks and thus protects these systems from potential production downtimes, data loss, image loss, etc. and the associated financial risks. A combination of automatic detection and the use of expert knowledge ensures the fastest possible detection of various attack scenarios. If there is a detected, active threat to the client‘s infrastructure, the measures contractually agreed individually with the client come into force immediately. The SOCaaS of the Certified Security Operations Center GmbH (CSOC) consists of standard services (core services) and optional services. These consist of the following:

- IT monitoring, technical review, verification and quality assurance of your alarms by the control centre
- Active response
- Auto escalation

The SOCaaS is divided into three **SERVICE MODULES**. All are part of the portfolio, they belong together for holistic monitoring. Each of the modules can be launched individually. During onboarding, the client decides which of the modules will be activated for monitoring. Activating all available modules should always be the final step:

SOCaaS – modules of our holistic monitoring
Flexible and modular

INCOMING AND OUTGOING TRAFFIC → **EVENT-BASED**

- *ANOMALY DETECTION*
- *NETFLOW ANALYSIS*
- *MACHINE LEARNING - SUPPORT IN THE SCORING PROCESS*

EVENT DATA FROM FIREWALL, ENDPOINT SOLUTION, SWITCHES, ROUTERS → **EVENT-BASED**

- *FURTHER ANALYSIS OPTIONS THROUGH INCORPORATION OF THE DATA*

EVENT DATA OF CLIENTS AND SERVERS → **SYSTEM-BASED**

- *SYSTEM AND PROCESS MONITORING*
- *SIEM*
- ***USE CASE*** *- BASED ANALYSIS BASED ON MITRE ATT&CK AND MACHINE LEARNING*

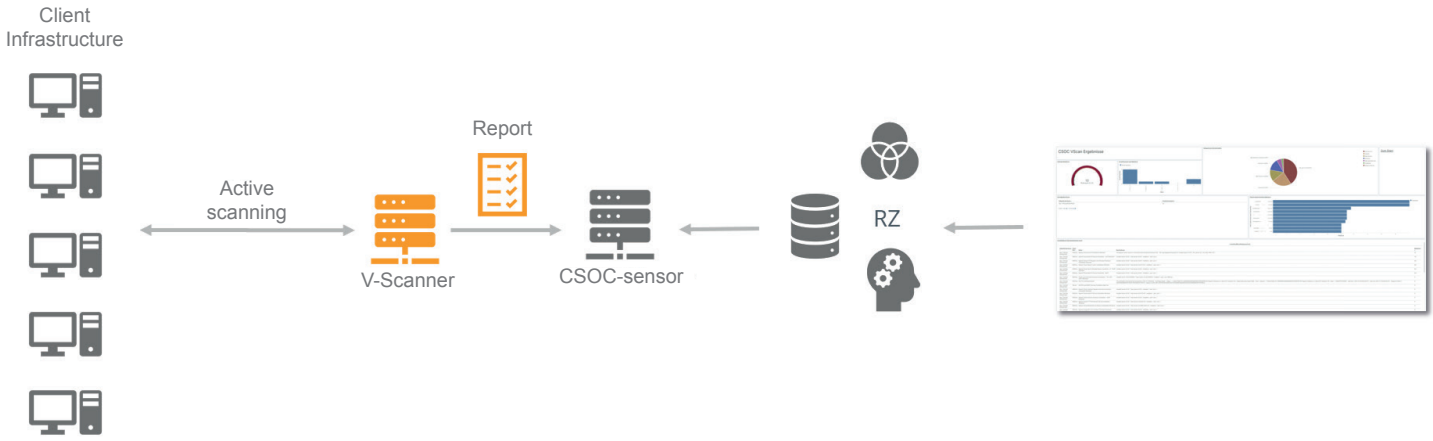
Technical monitoring is ALWAYS guaranteed with our SOCaaS 24x7. Based on the installed CSOC agents, our system automatically reports risk-weighted alarms around the clock.

Expandable performance components and flexibility

In addition, the SOCaaS includes the Active Response option and the Auto Escalation function. In the event of an attack, the system can intervene automatically if desired and take systems offline or block them (Active Response) as well as actively warn other systems (Auto Escalation). For further support, including personnel support in the event of an attack, our 24x7 control centre service and incident response service can be additionally booked. The optional V-Scanner (vulnerability scanner) actively examines the specific target systems for actual vulnerabilities in relation to the operating system, services and configurations.

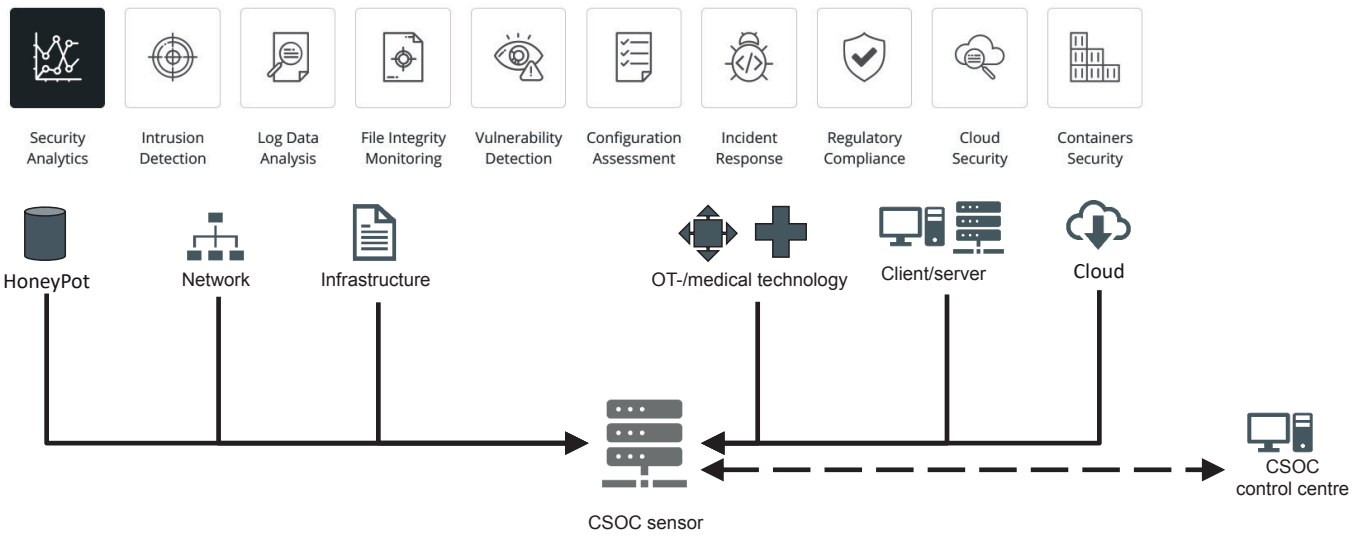
V-Scanner connection to SOCaaS

Active vulnerability management for your IT systems



Event channels of the SOCaaS

Both the classic active components of the IT environment and various control systems from the OT area (OT-SOCaaS) can be used as event channels of the SOCaaS. This also underlines the extremely high scalability of the SOCaaS:

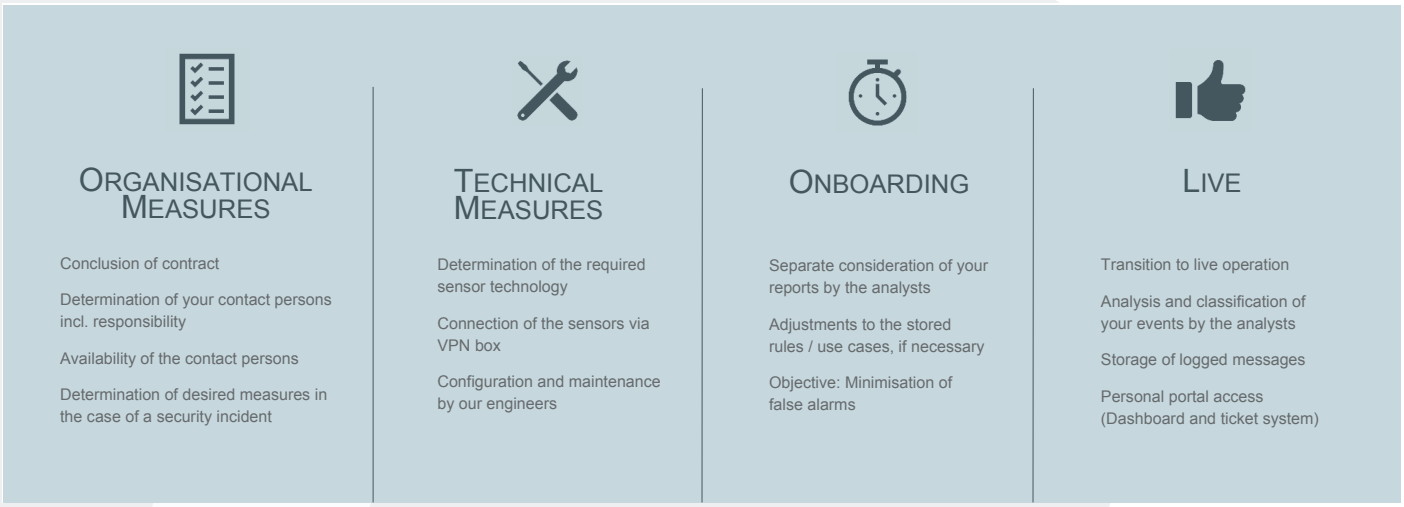


Implementation and use of SOCaaS

Which of your systems and which pre-defined threshold value this service should apply to is determined individually together during the onboarding process. Both the severity of your system and the exact definition of the respective use case play an important role. The introduction and use of SOCaaS is divided into the following stages:

Connection to SOCaaS

The connection stages



CSOC history

The CSOC was founded under the banner of the auditing and tax consultancy company dhpg Dr. Harzem & Partner mbB (dhpg), where it was operated under the name Cyber Security Operations Center. With more than 600 employees, dhpg, as an interdisciplinary company, provides support to clients such as family businesses and medium-sized enterprises, large companies, public sector administrations, non-profit organisations and private individuals, and employs auditors, tax advisors, lawyers and IT specialists. At the beginning of 2021, dhpg and the Cologne-based TÜV TRUST IT GmbH, TÜV AUSTRIA Group (TÜV TRUST IT) entered into a joint venture, already having established itself on the market as an independent partner for consulting and certification services relating to information security and data protection. The company consistently employs experienced, certified experts, auditors and IS auditors. It is certified for IS auditing, consulting and penetration tests by the Federal Office for Information Security (BSI) and therefore subject to permanent independent control.

The service portfolios of TÜV TRUST IT and dhpg now complement each other ideally in order to position future-oriented solutions on the market. TÜV TRUST IT as an independent consultant for information security and dhpg with its knowledge of confidential and protectable data.

Today, the SOC operates under the name **CERTIFIED SECURITY OPERATIONS CENTER (CSOC)** at a new state-of-the-art location in Bornheim, where, in addition to onboarding and monitoring of customer infrastructures, a great deal of emphasis is placed on the customer-oriented further development of the CSOC.

In the context of digitalisation, not only the challenges of defending against cybercrime are increasing above average, but also regulatory requirements such as the IT Security Act 2.0. The aim is therefore to continue expanding the CSOC‘s performance and to align it with current requirements, in order to become the leading SOC for medium-sized companies in Germany.

Bundling of IT security competences → CSOC

CERTIFIED SECURITY OPERATIONS CENTER GMBH
Adenauerallee 45-49 · D-53332 Bornheim
Phone: +49 2222 99222-0 · info@csoc.de

CSOC
dhpg & TÜV AUSTRIA Group