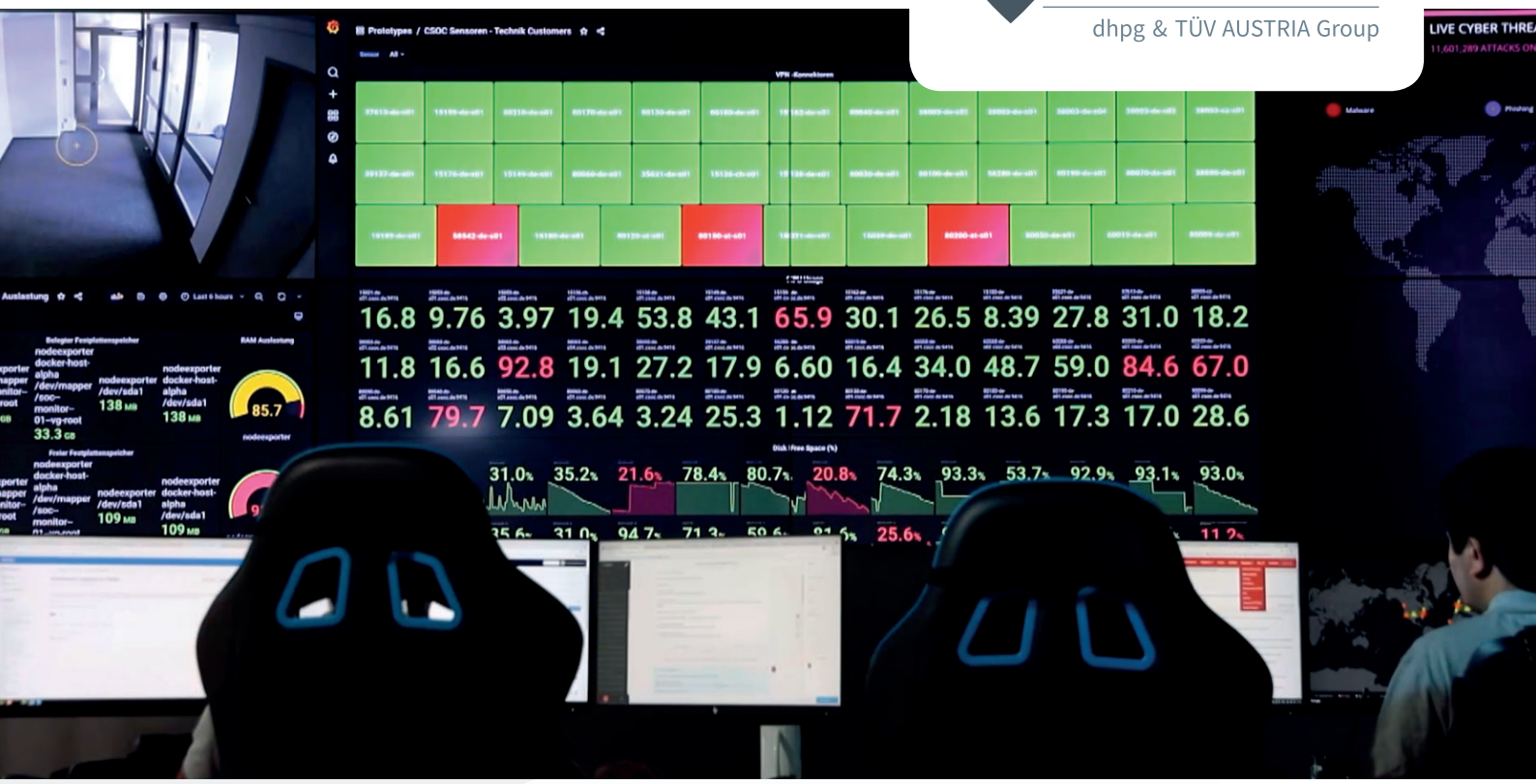
dhpg & TÜV AUSTRIA Group



CERTIFIED SECURITY OPERATIONS CENTER GmbH (CSOC)

SOC as a Service

SOCaaS – die Kernleistung des CSOC

Das SOC as a Service überwacht die IT-Systeme des Auftraggebers auf mögliche Cyberangriffe und schützt diese somit vor eventuellen Produktionsausfällen, Datenverlusten, Imageschäden etc. und damit verbundenen finanziellen Risiken. Eine Kombination aus automatischer Erkennung und dem Einsatz von Expertenwissen gewährleistet eine schnellstmögliche Detektion verschiedener Angriffsszenarien. Sollte eine erkannte, aktive Bedrohung der Infrastruktur des Auftraggebers vorliegen, treten umgehend die vertraglich individuell mit dem Auftraggeber vereinbarten Maßnahmen in Kraft. Das SOCaaS der Certified Security Operations Center GmbH (CSOC) besteht aus Standardleistungen (Kernleistungen) sowie aus optionalen Leistungen. Diese setzen sich wie folgt zusammen:

- IT-Monitoring, technische Überprüfung, Verifizierung und Qualitätssicherung Ihrer Alarme durch die Leitstelle
- Active Response
- Auto Escalation

Das SOCaaS ist in drei **LEISTUNGSBAUSTEINE** aufgeteilt. Alle drei Bausteine sind Bestandteil der Leistung, sie gehören für eine ganzheitliche Überwachung zusammen. Jeder der Bausteine kann einzeln ausgeführt werden. Während des Onboardings entscheidet der Kunde, welcher der Bausteine für die Überwachung aktiviert wird. Ziel ist immer alle verfügbaren Bausteine zu aktivieren:

SOCaaS – Bausteine unserer ganzheitlichen Überwachung
Flexibel und modular

Ein- und ausgehender Datenverkehr → **Eventbasiert**
- *Anomalie-Erkennung*
- *NetFlow-Analyse*
- *Machine Learning - Unterstützung im Scoring-Verfahren*

Eventdaten aus Firewall, Endpoint-Lösung, Switchen, Routern → **Eventbasiert**
- *Weiterführende Analysemöglichkeiten durch Kollaboration der Daten*

Eventdaten von Clients und Servern → **Systembasiert**
- *System- und Prozessüberwachung*
- *SIEM*
- ***USE CASE** - basierte Analyse auf Basis von MITRE ATT&CK und Machine Learning*

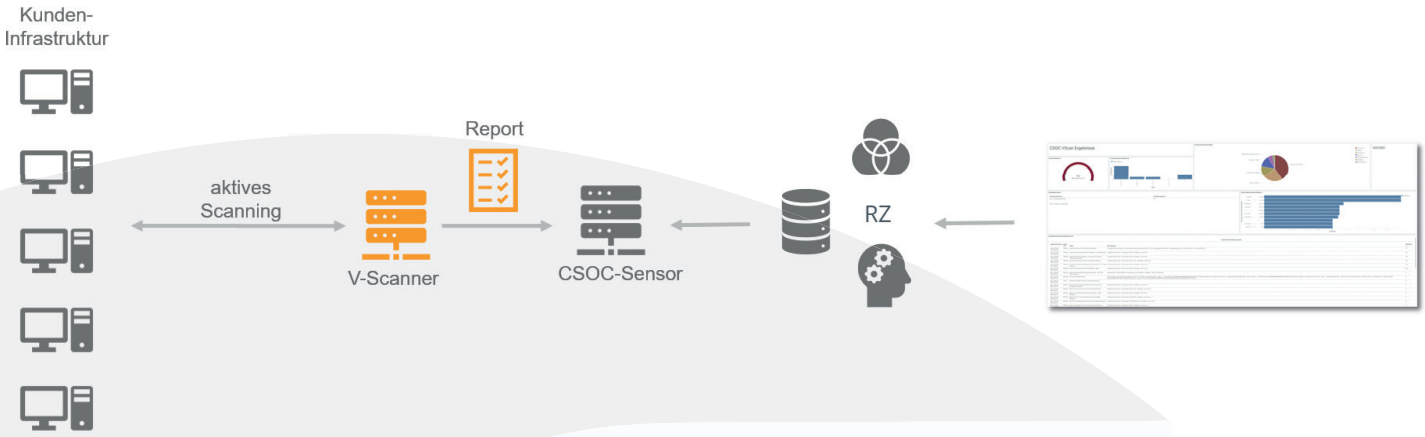
Die technische Überwachung ist bei unserem SOCaaS 24x7 **IMMER** gewährleistet. Unser System weist auf Basis der installierten CSOC-Agents automatisiert und rund um die Uhr die gewichteten Alarme aus.

Erweiterbare Leistungskomponenten und Flexibilität

Ergänzend beinhaltet das SOCaaS die Option des Active Response sowie die Auto Escalation Funktion. Damit kann das System im Falle eines Angriffs auf Wunsch automatisch einschreiten und Systeme vom Netz nehmen oder sperren (Active Response) sowie andere Systeme aktiv warnen (Auto Escalation). Für die weitere, auch personelle Unterstützung im Angriffsfall kann unser 24x7 Leitstellenservice und Incident Response Service ergänzend hinzugebucht werden. Der ebenfalls optionale V-Scanner (Schwachstellenscanner) untersucht Ihre Zielsysteme aktiv auf tatsächlich vorhandene Schwachstellen in Bezug auf Ihr Betriebssystem, die Services und Konfigurationen.

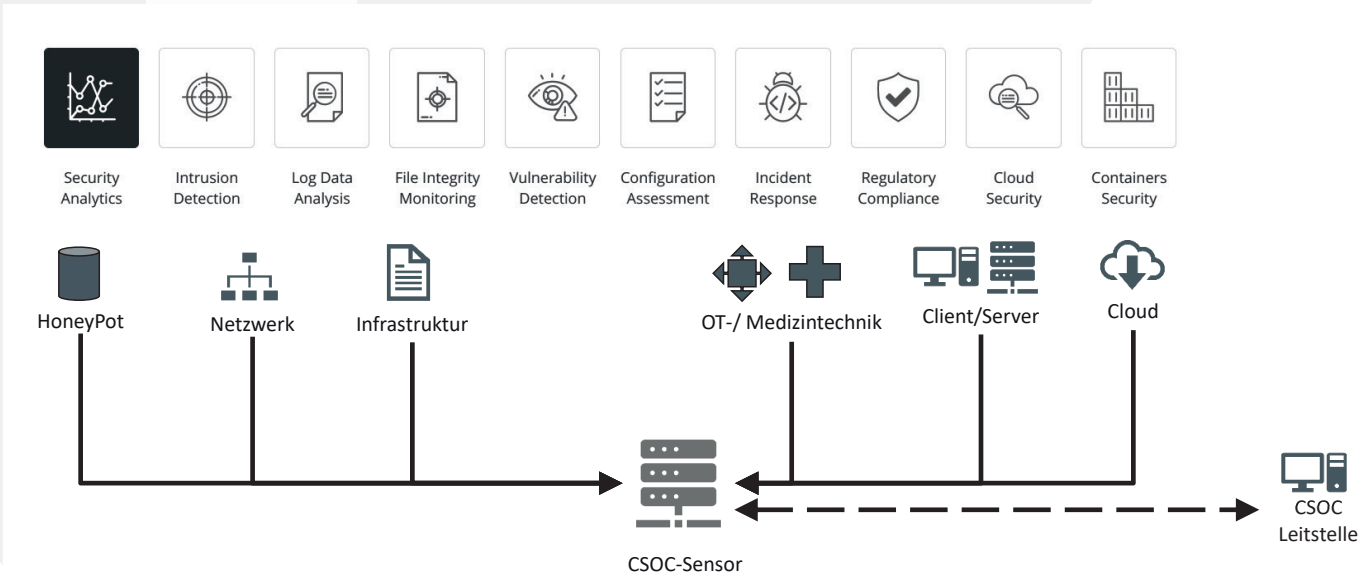
V-Scanner-Anbindung an SOCaaS

Aktives Schwachstellen-Management für Ihre IT-Systeme



Eventkanäle des SOCaaS

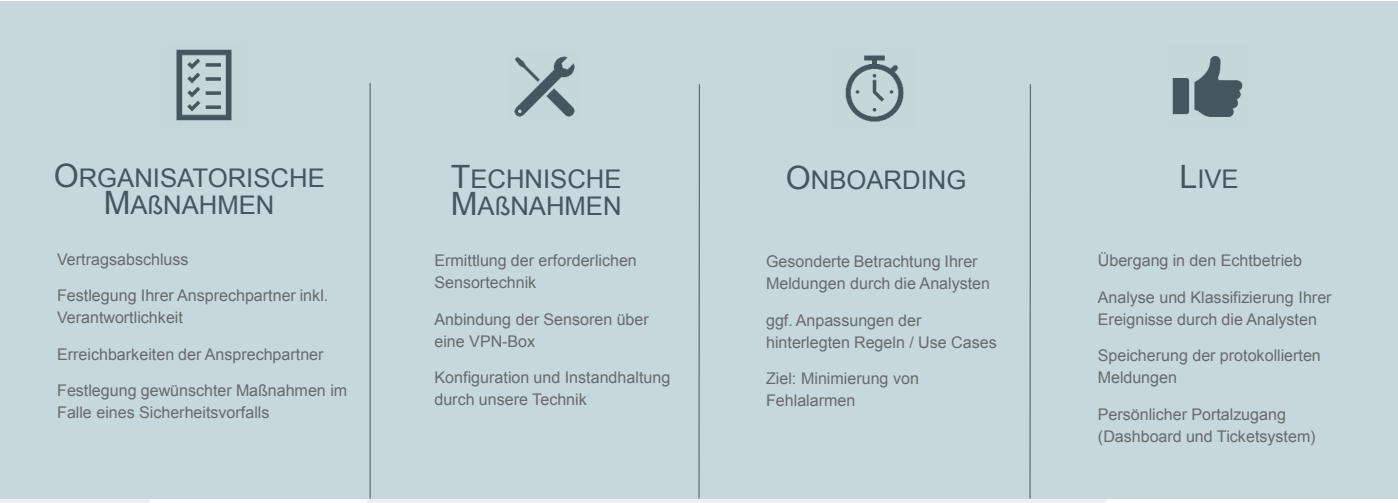
Als Eventkanäle des SOCaaS können sowohl die klassischen aktiven Komponenten der IT-Umgebung als auch diverse Steuerungssysteme aus dem OT-Bereich (OT-SOCaaS) herangezogen werden. Auch das unterstreicht die extrem hohe Skalierung des SOCaaS:



Implementierung und Nutzung des SOCaaS

Für welche Ihrer Systeme und ab welchem Schwellwert dieser Service greifen soll, wird gemeinsam während des Onboardings individuell festgelegt. Dabei spielen sowohl die Relevanz Ihres Systems als auch die genaue Definition des jeweiligen Use Cases eine wichtige Rolle. Die Einführung und Nutzung des SOCaaS ist in folgende Phasen aufgeteilt:

Anbindung an SOCaaS
Die Anbindungsphasen



CSOC – Historie

Seine Geburtsstunde erlebte das CSOC unter dem Dach der Wirtschaftsprüfungs- und Steuerberatungsgesellschaft dhpg Dr. Harzem & Partner mbB (dhpg), wo es unter dem Namen Cyber Security Operations Center betrieben wurde. Mit mehr als 600 Mitarbeitern unterstützt die dhpg als interdisziplinär arbeitendes Unternehmen die unterschiedlichsten Kunden wie Familienunternehmen und Mittelständler, Großunternehmen, Verwaltungen der öffentlichen Hand, gemeinnützige Organisationen und Privatpersonen und beschäftigt dabei Wirtschaftsprüfer, Steuerberater, Rechtsanwälte sowie IT-Spezialisten.

Anfang 2021 kam es schließlich zu einem Joint-Venture der dhpg und der Kölner TÜV TRUST IT GmbH Unternehmensgruppe TÜV AUSTRIA (TÜV TRUST IT), die sich bereits als unabhängiger Partner für Beratungs- und Zertifizierungsleistungen rund um die Themen Informationssicherheit und Datenschutz am Markt etablieren konnte. Das Unternehmen setzt durchgängig erfahrene, zertifizierte Experten, Auditoren und IS-Revisoren ein und unterliegt als vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierter IT-Sicherheitsdienstleister für

IS-Revision und IS-Beratung sowie IS-Penetrationstests einer dauerhaften unabhängigen Kontrolle. So ergänzen sich nun die Leistungsportfolios der TÜV TRUST IT und der dhpg ideal, um zukunftsorientierte Lösungen am Markt zu positionieren – die TÜV TRUST IT als unabhängiger Berater für Informationssicherheit und die dhpg mit ihrem Wissen um vertrauliche und schützenswerte Daten.

Fortan operiert das SOC unter der Bezeichnung **CERTIFIED SECURITY OPERATIONS CENTER (CSOC)** an einem neuen, hochmodern ausgestatteten Standort in Bornheim, wo neben dem Onboarding und Monitoring der Kundeninfrastrukturen auch auf die kundenorientierte Weiterentwicklung des CSOCs viel Wert gelegt wird.

Im Zuge der Digitalisierung steigen nicht nur die Herausforderungen zur Abwehr der Cyber-Kriminalität überproportional, sondern auch regulative Vorgaben wie beispielsweise durch das IT-Sicherheitsgesetz 2.0. Ziel ist es daher, die Leistungsfähigkeit des CSOCs weiterhin stetig auszubauen und an den aktuellen Anforderungen auszurichten, um das führende Mittelstands-SOC Deutschlands zu werden.

Bündelung von IT-Security Kompetenzen → CSOC

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

CSOC
dhpg & TÜV AUSTRIA Group