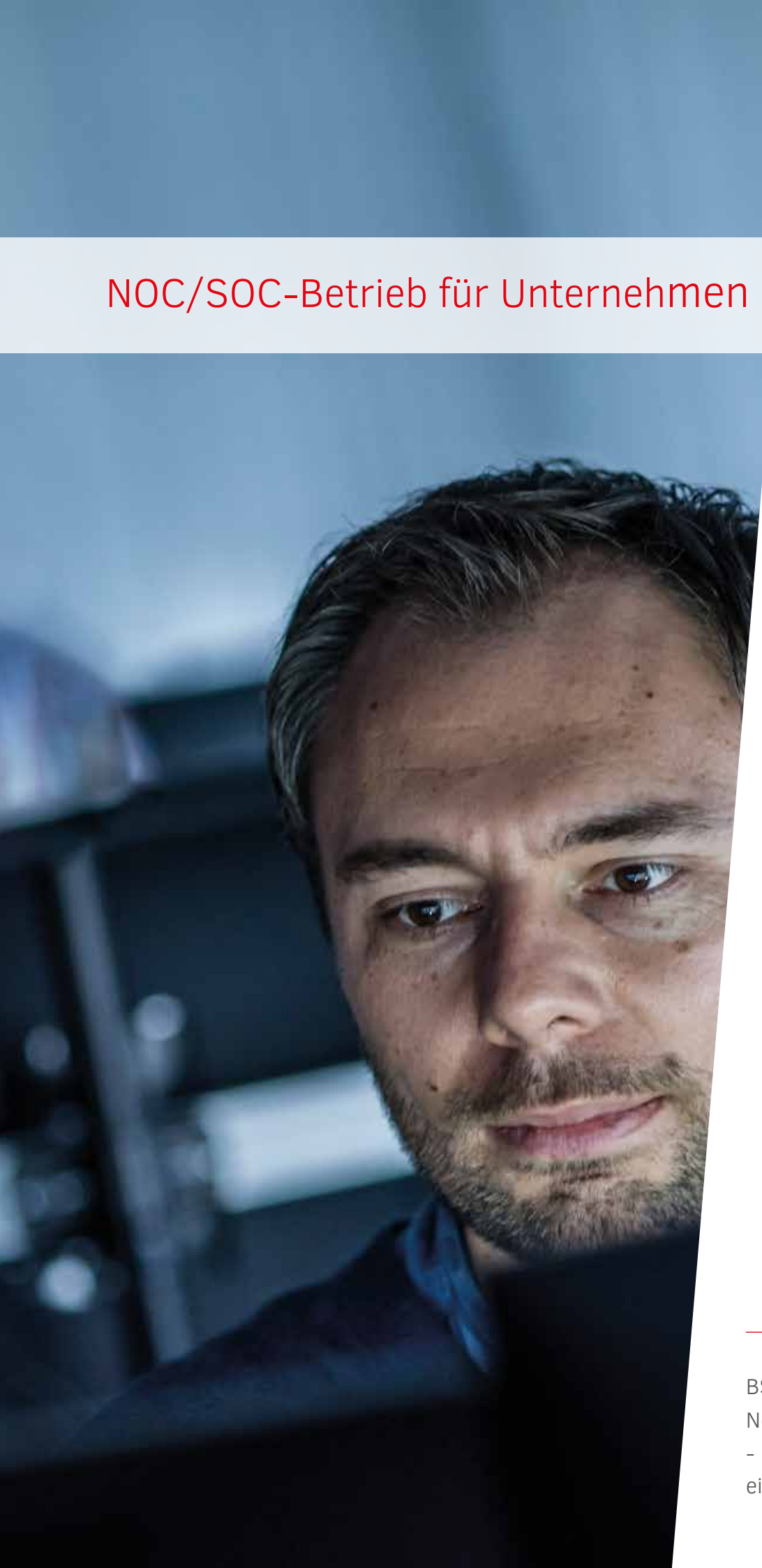
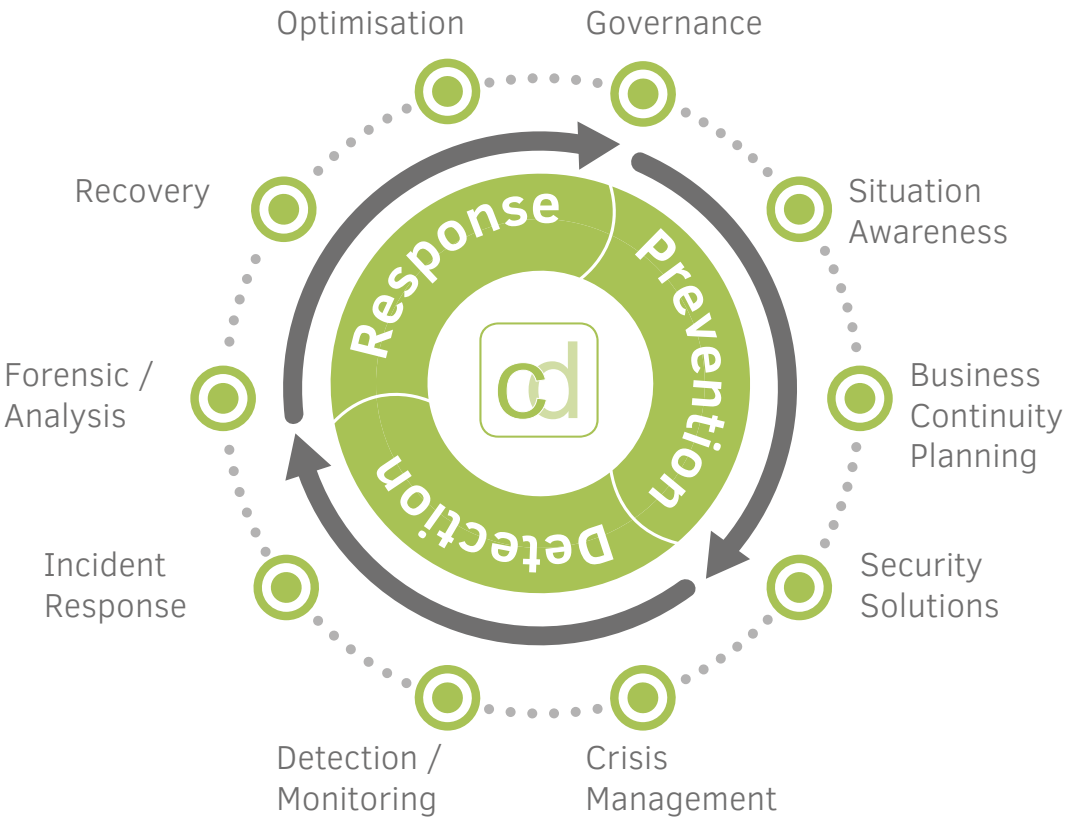
dacoso
data communication solutions

NOC/SOC-Betrieb für Unternehmen



BSI-zertifizierte
Netzwerk-Überwachung*
- ohne Investition und
eigenes Personal

Im Fokus: Cyber Defence



Geschützte IT-Infrastrukturen sind heute für alle Unternehmen wichtig – keiner kann sich hier Lücken leisten. Behörden und sicherheitsbetreute Unternehmen haben sogar überdurchschnittlich hohe Anforderungen zu erfüllen.

Wenn ein Datenangriff öffentlichkeitswirksam passiert, erhöht das kurzzeitig die Sicherheitsaktivitäten: IT-Verantwortliche in den Unternehmen prüfen die entsprechenden Einschlupflöcher und schließen sie bei Bedarf so schnell wie möglich. Doch für die Abwehr von Datensabotage reichen isolierte Maßnahmen heute keineswegs mehr aus.

* BSI ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

Network & Security Operation Center

Im Zentrum unserer Lösungen für Cyber Defence steht ein hochmodernes NOC/SOC, von dem aus wir Ihre Hardware und Verbindungen kontinuierlich überwachen. Ausgangspunkt dabei ist immer die Prävention: Machine-Learning, Künstliche Intelligenz und Detektionsmöglichkeiten verzahnen wir so, dass Gefahren früh erkannt werden.

Security Analyse Tools identifizieren Bedrohungen von Netzwerken, Systemen, Applikationen und Services rechtzeitig, sprechen konkret Empfehlungen für effektive Gegenmaßnahmen aus und liefern wiederum wichtige Erkenntnisse zur gezielten Vorbeugung – als Grundlage für den besten Schutz Ihrer Unternehmenswerte. Insbesondere bei heterogenen Systemen erfordert das nicht nur die richtige und leistungsfähige Kontroll-Plattform, sondern auch geschultes Fachwissen: Experten, die Probleme realistisch einschätzen und die nächsten Schritte mit Besonnenheit angehen. Dafür bringen wir unsere Expertise als MSSP (Managed Security Service Provider) ein, die bis hin zur forensischen Analyse im Nachgang eines Hacker-Angriffs reicht.

Ist die Infrastruktur leistungsstark und stabil, laufen Angriffe schneller ins Leere. Entsprechend fahrlässig ist es, Geräte nicht auf dem benötigten Stand zu halten. Die Hardware auch mal kurzfristig zu aktualisieren, ist im laufenden Betrieb einer IT-Abteilung jedoch nicht einfach. Mit Maintenance- und Update-Funktionen unterstützen wir Sie in genau dem Maße, wie Sie uns brauchen. Parallel übernehmen wir auf Wunsch die permanente Überwachung der Geräte, mit stets aktueller Status-Dokumentation. Dadurch werden Ausfälle sofort erkennbar und größere Schäden vermeidbar. Sollte es dennoch zu Netzwerk-Vorfällen kommen, leiten wir umgehend die Fehler-Behebung ein.

Beispiele NOC

- Service-Monitoring von Netzwerk-Komponenten auf Basis einer SNMP-Überwachungslösung (ADVA Optical Networking)
- Service-Monitoring für WAN-Optimizer (Ipanema)
- Service-Monitoring für Verschlüsselungs-Lösungen mit BSI-Zulassung (SINA Layer-3-Boxen, ADVA Optical Networking, atmedia) inkl. Verwaltung und Versand der Chip-Karten sowie Betrieb des zentralen Verwaltungs-Servers

Mit unseren SOC-Funktionen treten wir den Problemen entgegen, die nicht gerätever-schuldet sind. Cyber-Kriminelle finden immer neue Einfallstore. Wir kontrollieren, ob verdächtige Aktivitäten im Inneren Ihres Netzwerkes stattfinden. Über die intelligente Plattform unseres Technologie-Partners finally safe hat unsere SOC-Mannschaft gefährliche Anomalien umgehend auf dem Bildschirm. Sollte sich das Problem nicht direkt abwenden lassen, kümmern wir uns darum, dass die Systeme sofort wiederhergestellt werden. Damit der Schaden gering bleibt, muss das schnell passieren. In einer forensischen Schwachstellen-Analyse zielen wir anschließend darauf ab, weitere Versuche dieses Angriffmusters präventiv abzublocken.

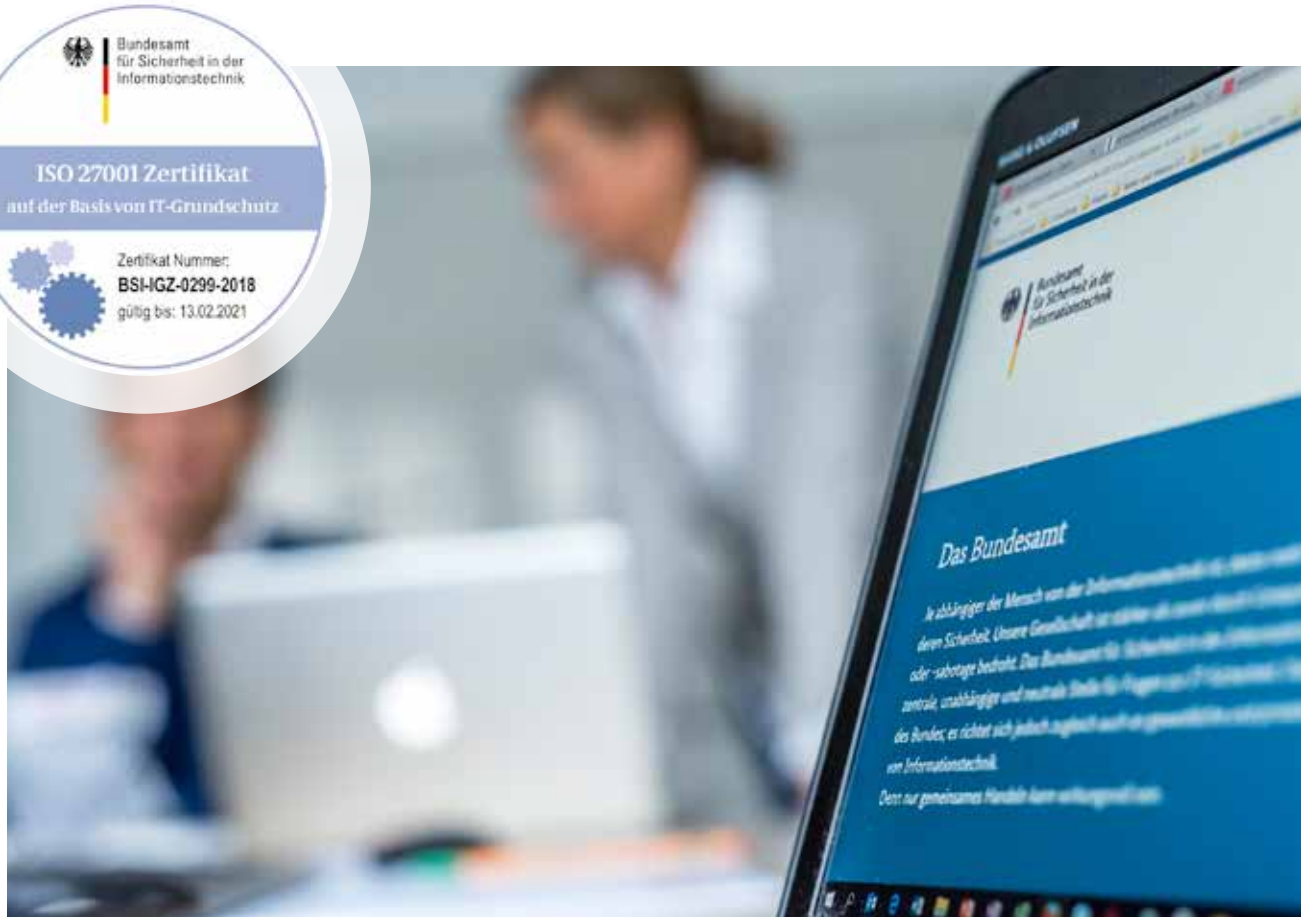
Beispiele SOC

- Alarmierung bei Auffälligkeiten (Frühwarn-System von finally safe)
- Orchestrierung, Automatisierung und Reaktion auf Vorfälle in Echtzeit mit unserer Security-Information- und Event-Management-(SIEM)-Plattform (LogPoint)
- Next Generation End Point Security mit Künstlicher Intelligenz (CylancePROTECT)
- Asset & Device Management für Network Access Control (macmon)
- Zwei-Faktor-Authentifizierung
- komponentenbezogene Schwachstellenanalyse, Prevention (über Penetration Testing)
- Unterstützung beim Restore der Systeme

Abwehr und Prävention

Die dacoso NOC/SOC-Vorteile auf einen Blick

- 24/7 bedienter Betrieb
- alle Services bei Bedarf gemäß den hohen Anforderungen des BSI
- modulares Konzept: NOC/SOC-Dienste sind frei wählbar
- Hochsicherheitscontainer für alle Überwachungs-Server und Netzwerk-Komponenten
- optionaler NOC-Support im Fehlerfall: von telefonischer Beratung bis hin zur Ersatzteil-Lieferung
- NOC/SOC-Management von Deutschland aus, mit hier ausgebildeten Technikern
- durchgängig deutschsprachiger Support, bei Bedarf auch in Englisch



ISO 27001-Zertifikat IT-Grundschutz

Dass wir unsere Aufgaben verantwortungsvoll erfüllen, zeigt die Zertifizierung unseres NOC/SOC durch das Bundesamt für Sicherheit in der Informationtechnik (BSI). Mit dem „ISO 27001-Zertifikat auf Basis von IT-Grundschutz“ ist amtlich dokumentiert, dass wir für „Informationssicherheit und die erfolgreiche Umsetzung internationaler Normen unter Anwendung der IT-Grundschutz-Methodik nach innen und außen“ (BSI) sorgen. Für viele Unternehmen – darunter insbesondere sicherheitsbetreute Unternehmen sowie KRITIS-Versorger – ist das BSI-Siegel zwingende Voraussetzung für die Nutzung einer Sicherheitslösung.

dacoso bietet Connectivity-Lösungen für Rechenzentren und Netze und sorgt mit Cyber Defence für den Schutz der Datenkommunikation. Dafür liefert das Unternehmen die notwendige Hardware und kümmert sich mit zahlreichen Services darum, dass die Systeme leistungsstark und zuverlässig laufen. Mit seinen Cyber-Defence-Lösungen prüft und sichert dacoso die Netzwerke, so dass sie umfassend gegen Datenangriffe geschützt sind.

www.dacoso.com

KBR-NOC/SOC-D-1804 © Axel Boesten