T.I.S.P./T.P.S.S.E. Community Meeting 2026

Berlin, 10. - 11.11.2026

Erfahrungsbericht: Einführung eines gemanagten SOC inklusive der Einführung einer SIEM Software

Stefan Haibach, Philipp Rothmann

ITSG GmbH

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Agenda

1. **Herausforderung**: Beobachtbarkeit von Sicherheitsereignissen jenseits klassischer Malware
2. **Technische Lösung**: Wie funktioniert ein SIEM?
3. **Organisatorische Prozesse**: Wie arbeitet das SOC mit der ITSG zusammen?
4. **Einführung**: Nutzung der Lösung für ein Projekt oder eine Fachanwendung
5. **Best Practice**: Das sollten Sie bei der Einführung beachten


ITSG GESAMTSYSTEM KRANKENVERSICHERTEN-NUMMER
ITSG TRUST CENTER
ITSG DAKOTA
Made in Germany !
ITSG PRIVATE PLATFORM
30 Jahre ITSG
SYSTEM UNTER-SUCHUNG
GKV INFO SHOP
Forum T
DATENSTELLEN
ITSG
GKV Datenschutz
SIEM / SOC
Informationssicherheit
BMG
BMAS
Berlin
Rechenzentrum 1
Rechenzentrum 2
Flexible Datendrehscheibe
in
out
Verzeichnisse und Basisdaten
Statistik-Küche
ITSG GKVNET CRYPT
SV-MELDEPORTAL® ARBEITGEBER SOZIALVERSICHERUNG
Software-Entwicklung
INFORMATIONSPORTAL ARBEITGEBER SOZIALVERSICHERUNG
Fachkonzept-Schmiede
KOHLE
KONZE
Frankfurt/Main
Atelier RAP
GKV-KOMSERVER
Müller & Co.KG
Offenbach
ITSG
Daten-Auto-bahn
Pflegeheim
Strategie & Standards
Schülke 2026

Herausforderung: Regulatorische Anforderungen erfüllen

ISO 27001
- Vorfalls-Management-Prozess
- Logging, Monitoring & Threat Intelligence technisch gewährleistet

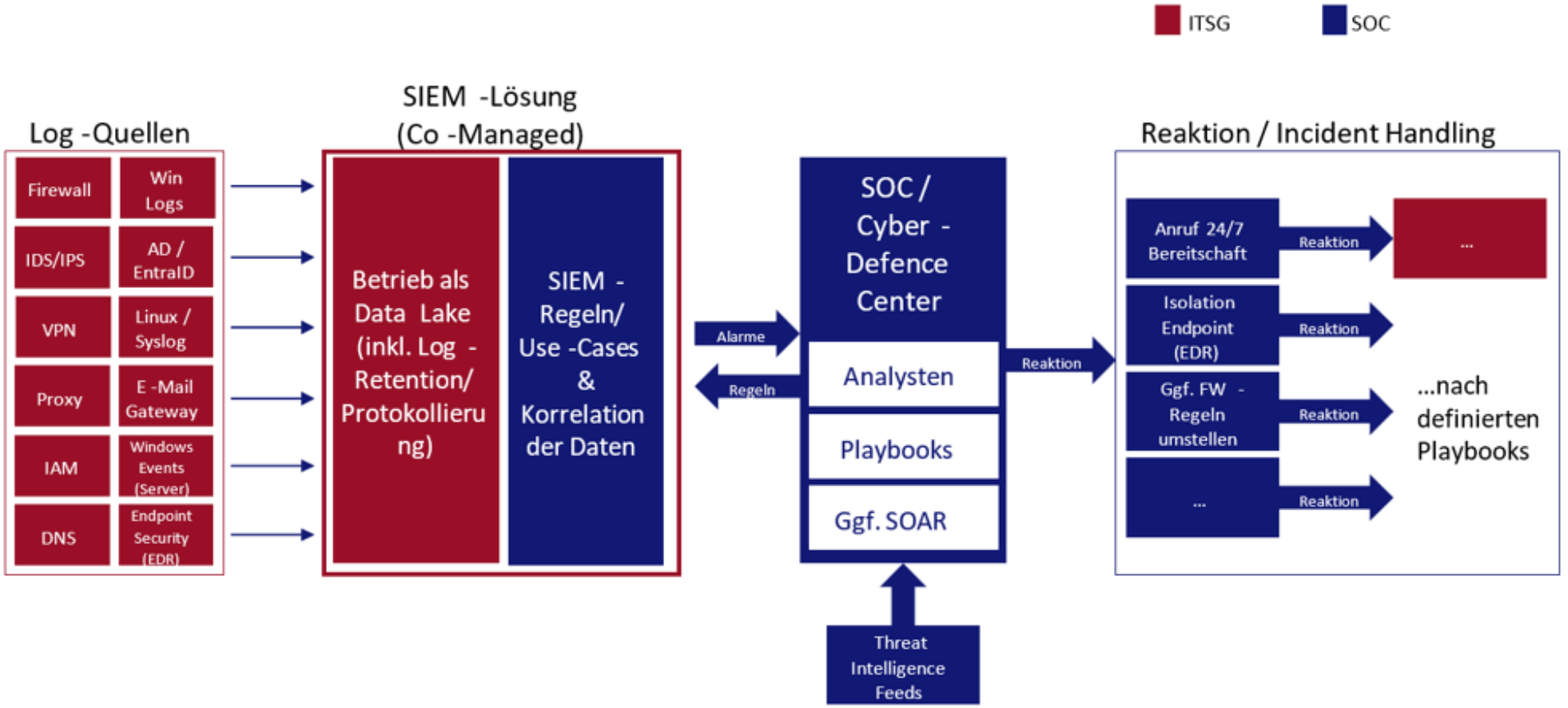
KRITIS
- Systeme zur Angriffserkennung nach Stand der Technik
- Kontinuierliche 24-Stunden Überwachung
- Automatische Identifikation von Bedrohungen

BSI C5:2026
- SIEM als harte Anforderung für Cloud Anbieter
- Nachweis einer kontinuierlichen Sichtung der Logs auf Sicherheitsereignisse
- Relevante Logs in unveränderbarer Form vorgehalten

NIS2
- Zwingt zu hoher Detection-Reife, um Meldepflichten einzuhalten
- Macht Systeme zur Angriffserkennung ebenfalls zur Pflicht
- Managementverantwortung: SIEM wird „Chefsache“

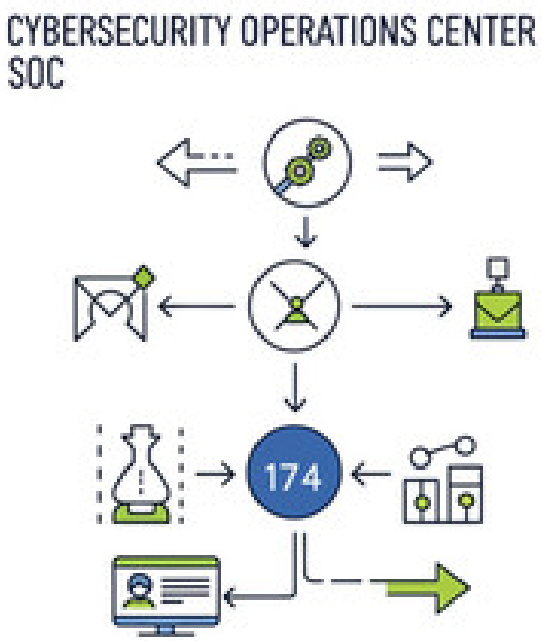


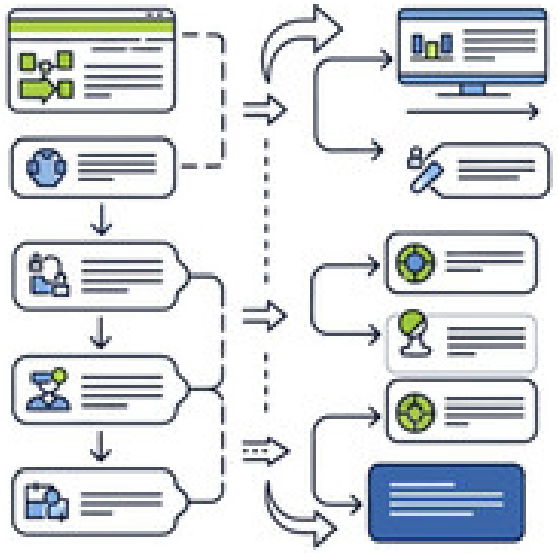
SIEM: Co-Managed Platform



Was ist ein Security Operation Center?

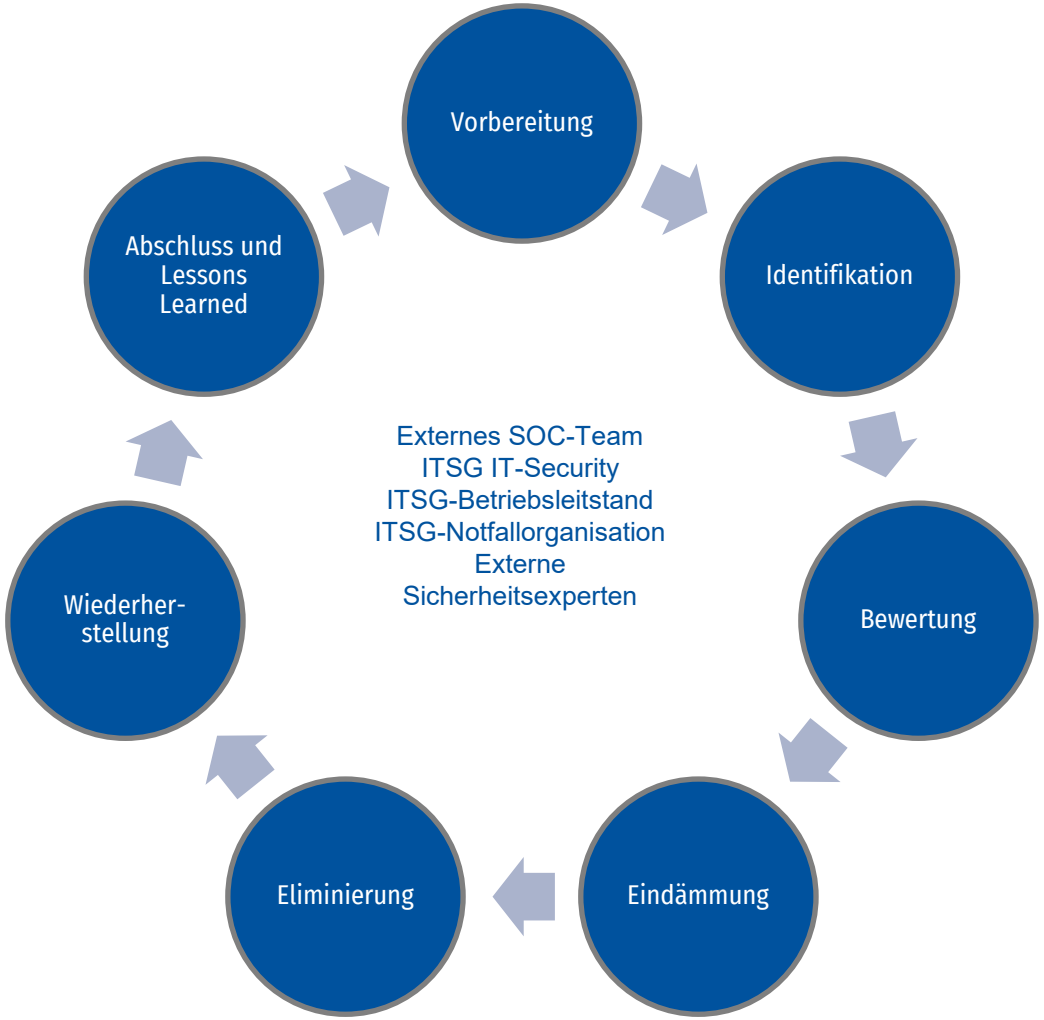
- Menschliche Analysten, die auf Basis des SIEMs 24/7 Alarme prüfen
- Mehrstufigkeit: initiale Triage von Alarmen durch Junior Analysten, definierte Eskalationsstufen
- Kombiniert verschiedene Analysewerkzeuge: KI-Tools, Log Korrelation, Threat Intelligence
- Klar definierte Prozesse und Schnittstellen zum Kunden und zu Incident Respondern



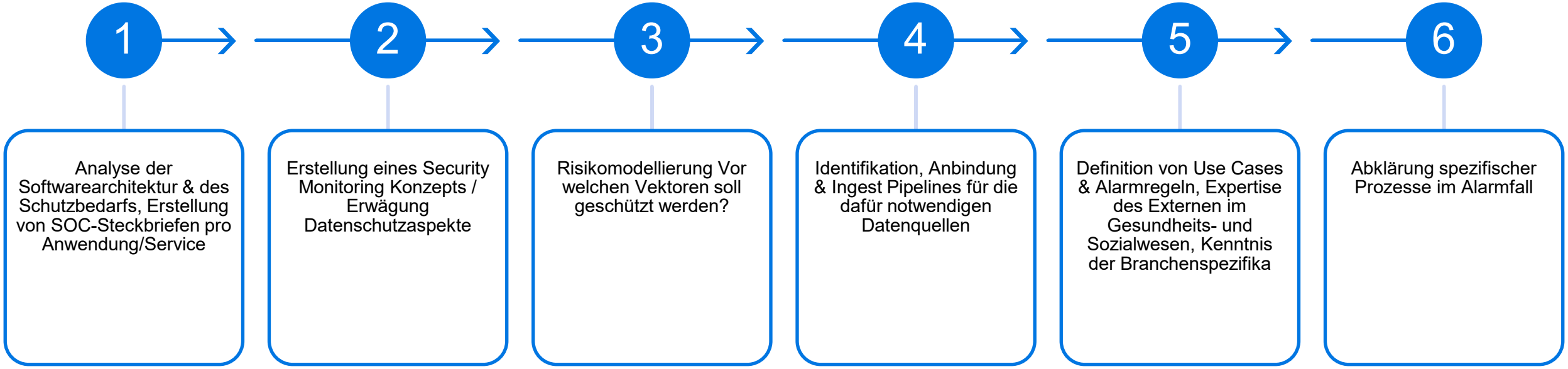


Quelle: Adobe Stock

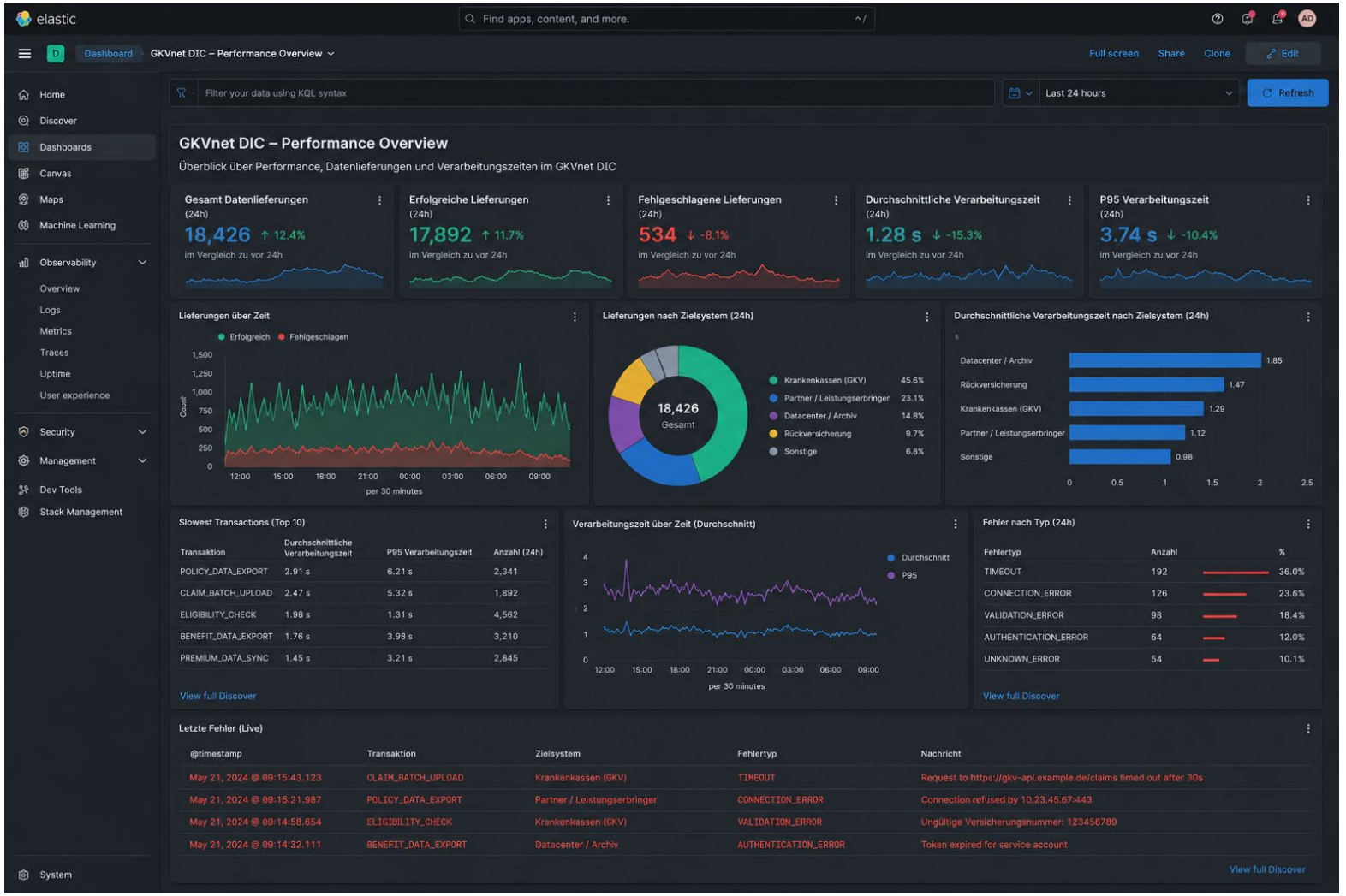
Organisatorischer Aufbau – Klare Verantwortlichkeiten



Einführung eines SIEM/SOC-Systems für ein Produkt / einen Kunden / eine Fachanwendung



Das Ergebnis: Unser Dashboard



Compliance und Wertigkeit

- Ein SIEM/SOC-Center kostet Geld und Zeit.
- Kunden wie Belegschaft müssen den Wert dieser Detektion erkennen, denn ein Betrieb ohne SIEM/SOC ist im Ernstfall noch viel teurer (Schadensvermeidung).
- Eine zielgruppengerechte Aufklärung ist daher essenziell.

Best Practice

Business as Usual reicht nicht

- Zusammenarbeit von externem SOC-Anbieter und Unternehmen muss eingespielt werden.
- Verantwortlichkeiten müssen eindeutig geklärt sein (z. B. Ansprechpartner müssen verlässlich erreichbar sein - auch nachts und an Wochenenden).
- Die Regeln im SIEM müssen immer zeitnah der aktuellen Bedrohungslage angepasst werden. Was vor einigen Wochen passte, kann heute schon (auch in Hinblick auf KI) unzureichend sein.
- Unser Kunde/Auftraggeber muss regelmäßig auf dem Laufenden gehalten werden.
- Es geht weiter…Einbindung des ITSM usw.

Vielen Dank für Ihr Interesse

Bei Fragen kontaktieren Sie uns gern



Stefan Haibach
Stefan.haibach@itsg.de
069-8700358-174



Philipp Rothmann
datenschutz@itsg.de
069-8700358-244