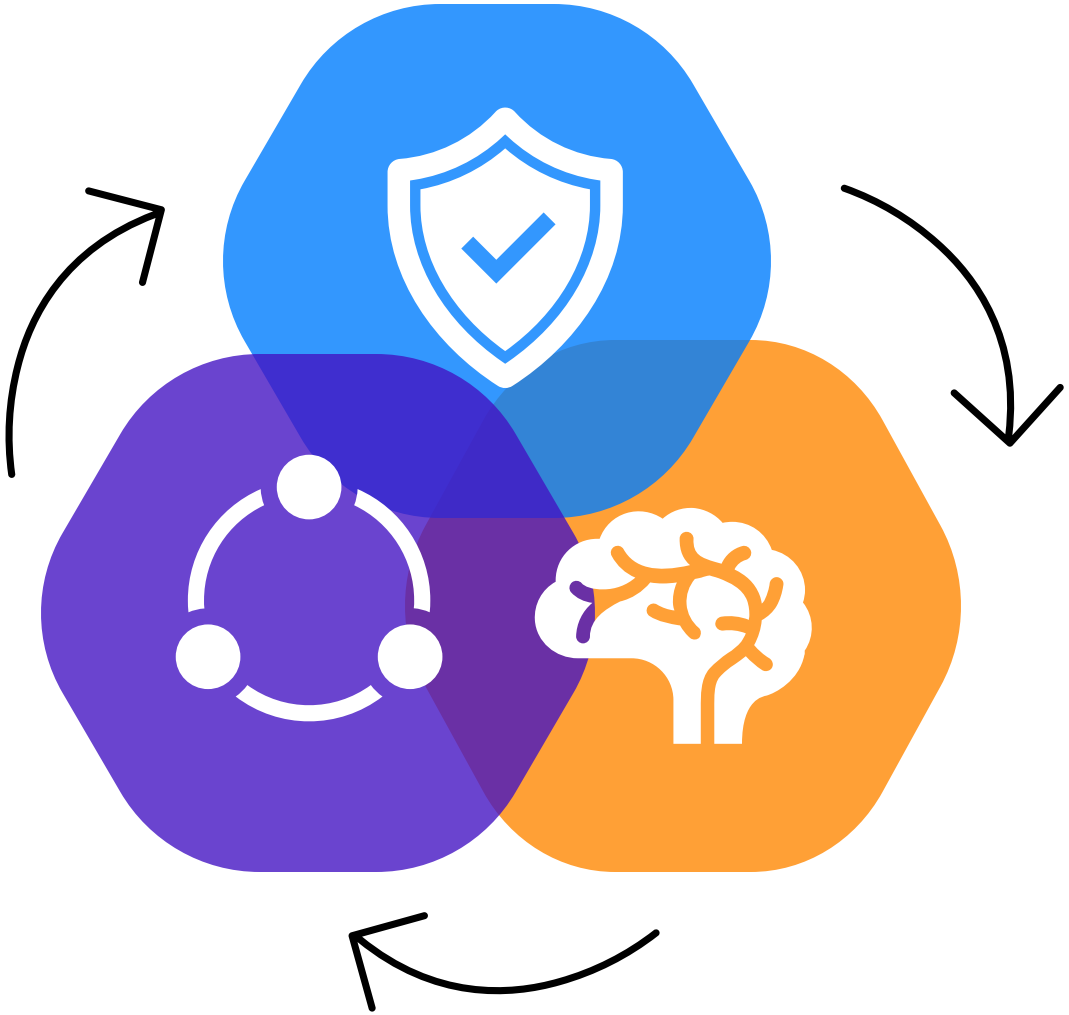
# SOFT-CONSULT

Wir beraten den Mittelstand.

Für digitale Lösungen mit Mehrwert.

Ihr Digitalisierungspartner



# SOFT-CONSULT SECURITY

**Managed Security Lösungen**

- Integrierte, ganzheitliche Sicherheit.
- Schutz über Endpunkte, Identitäten und Cloud hinweg.
- Künstliche Intelligenz und Machine Learning für proaktive Bedrohungserkennung.

SOFT-CONSULT

# INHALT

SOFT-CONSULT

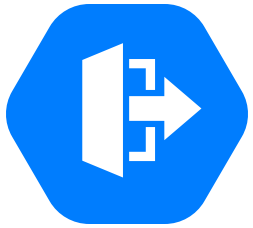
# KI nutzen – aber sicher: Was Unternehmen jetzt beachten sollten

# Warum Security bei KI wichtig ist

## KI schafft neue Sicherheitsanforderungen

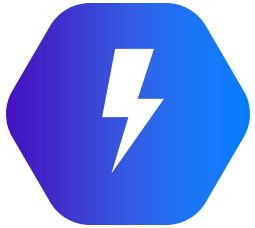
**Sensible Daten**

KI verarbeitet große Mengen sensibler Unternehmensdaten



**Interner Zugriff**

Ergebnisse basieren auf bestehenden Daten (→ Risiko von Datenabfluss)

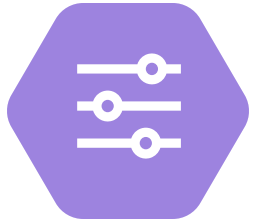


**Automatisierung**

Automatisierung erhöht die Geschwindigkeit, auch bei Angriffen

**Neue KI-Angriffe**

Neue Angriffsformen durch KI (Phishing, Social Engineering, Deepfakes)



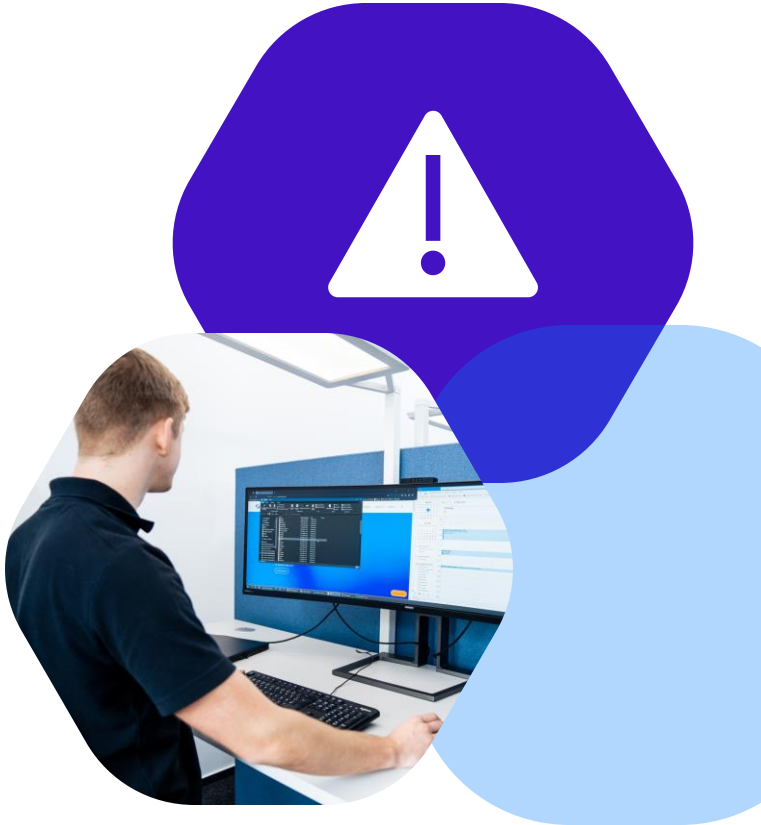
**Fehlkonfigurationen**

Fehlkonfigurationen können Risiken massiv verstärken

# Konkrete Risiken

## Typische Risiken bei der Nutzung von KI

- Ungewollte Preisgabe sensibler Informationen
- Zugriff auf Daten, die eigentlich nicht sichtbar sein sollten
- Fehlende Transparenz: Wer sieht was?
- Vertrauen in KI-Ergebnisse ohne Validierung
- Schatten-IT: Nutzung von nicht freigegebenen KI-Tools

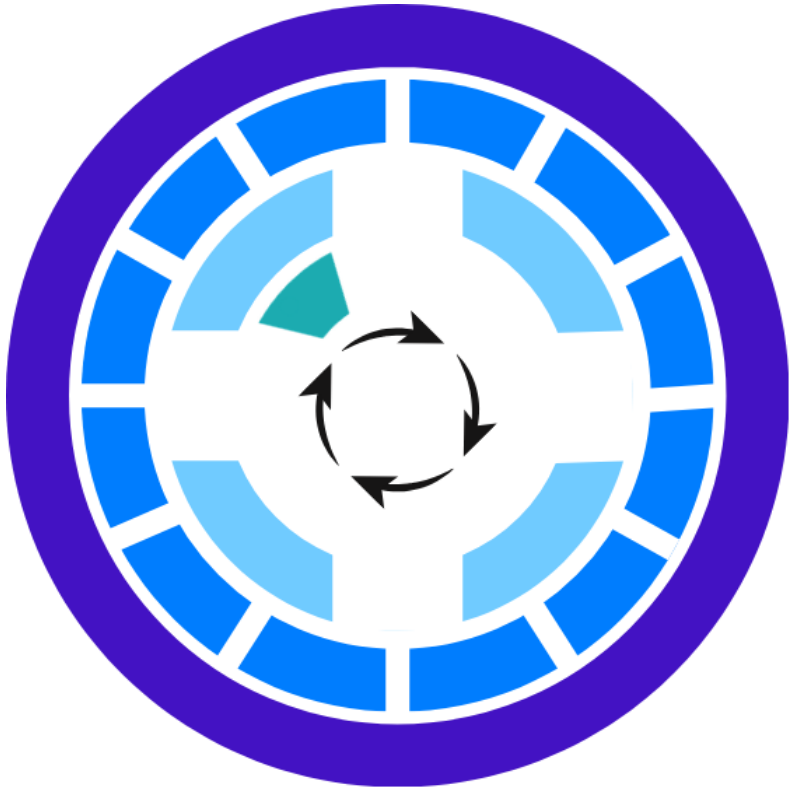


SOFT-CONSULT

# Wie sieht Ihr Security Lifecycle aus?

# Security Lifecycle

- Kein einmaliges Setup
- Bedrohungen verändern sich kontinuierlich
- Systeme, Nutzer und Daten entwickeln sich weiter
- Sicherheit muss daher dauerhaft betrachtet werden

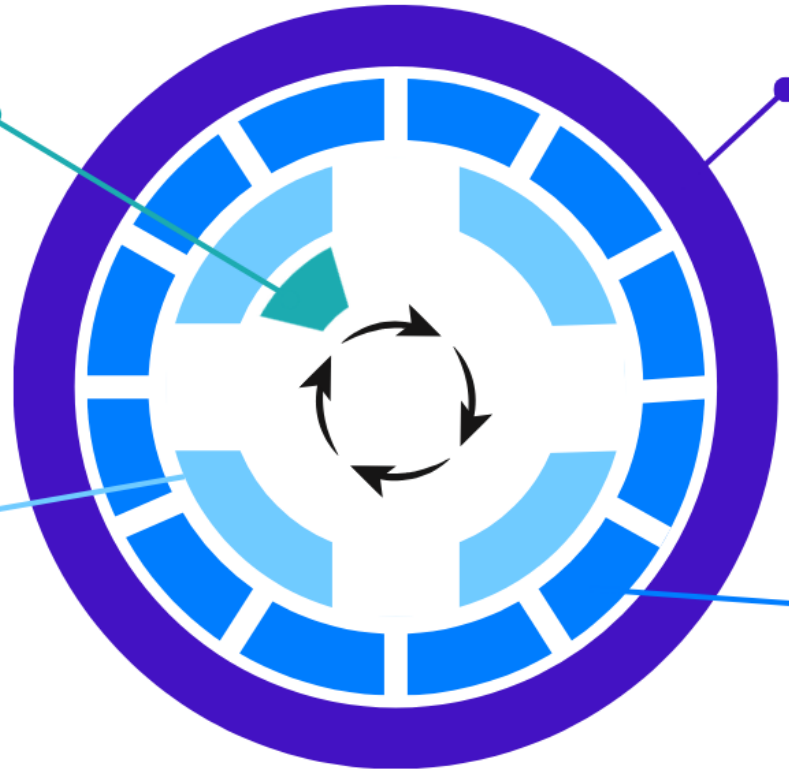


> ***IT-Sicherheit ist kein Projekt, sondern ein Prozess***

# Security Lifecycle

**Jährliche Maßnahmen**

- Review von Konzepten & Policies
- Management-Review & Priorisierung
- Pentesting



**Kontinuierliche Maßnahmen**

- Monitoring & Incident Detection
- Log- & Ereignisüberwachung
- Reaktion auf sicherheitsrelevante Vorfälle

**Maßnahmen pro Quartal**

- Schwachstellen-Scan (CVE-Scan)
- Admin-Check/Revision von Zugriffen & Rechten
- Test der Prozesse (Notfall- & Incident-Prozess)

**Monatliche Maßnahmen**

- Patchmanagement
- Review kritischer Erkenntnisse (Findings) Management-Report

# Security Prozess

**Erkennen** (Detection)

**Bewerten** (Analysis)

**Reagieren** (Response)

**Berichten** (Reporting)

# Security Prozess

**Erkennen** (Detection)

**1. Auffälligkeiten frühzeitig erkennen**

- Kontinuierliche Überwachung sicherheitsrelevanter Ereignisse
- Automatische Erkennung von Auffälligkeiten
- Fokus auf Endpunkte, Identitäten und Cloud

**Ziel: Risiken früh sichtbar machen**

# Security Prozess

**Bewerten** (Analysis)

## 2. Ereignisse richtig einordnen

- Unterscheidung zwischen echten Risiken und Fehlalarmen
- Kontextbasierte Analyse
- Priorisierung nach Kritikalität

# Security Prozess

**Reagieren** (Response)

**3. Kontrolliert reagieren**

- Klare Reaktionsprozesse bei Sicherheitsvorfällen
- Maßnahmen zur Schadensbegrenzung (z. B. Isolation von Systemen)
- Unterstützung bei Analyse und Behebung
- Strukturierte Incident Response

# Security Prozess

**Berichten** (Reporting)

**4. Transparenz schaffen und daraus lernen**

- Regelmäßige Berichte zu Sicherheitsereignissen
- Übersicht über Schwachstellen und Angriffe
- Bewertung des Sicherheitsniveaus
- Grundlage für kontinuierliche Verbesserung

# Was bedeutet das für Ihr Unternehmen?

- Security muss kontinuierlich betrieben werden
- Reaktion allein reicht nicht – ganzheitlicher Ansatz notwendig
- Kombination aus Technologie, Prozessen und Know-how
- Grundlage für moderne Managed Security

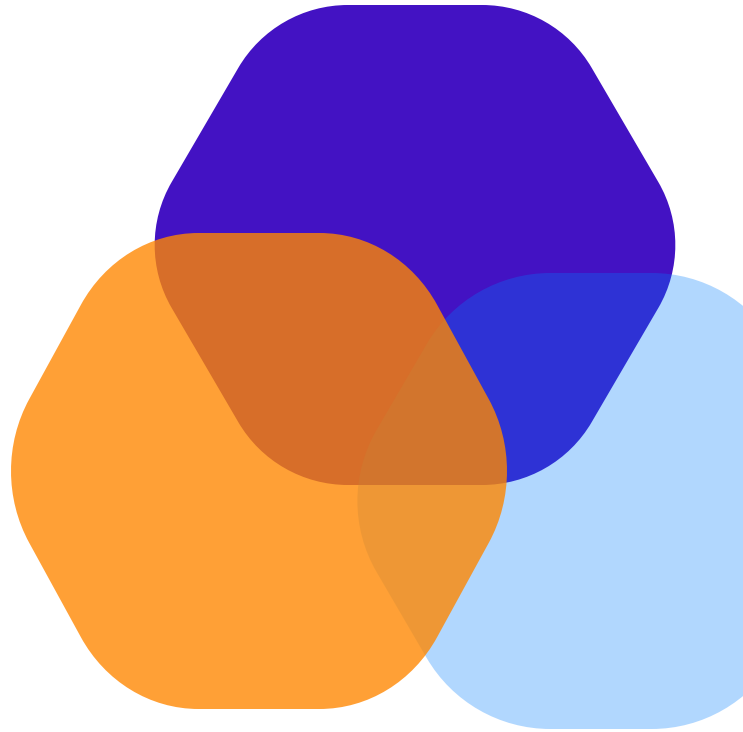
# Warum klassische Security heute nicht mehr ausreicht

- Fokus auf einzelne Systeme statt Gesamtumgebung
- Reaktive Ansätze (erst handeln, wenn etwas passiert)
- Signaturbasierte Erkennung greift zu kurz
- Neues Angriffsverhalten: automatisiert, dynamisch, KI-gestützt
- Fehlende Transparenz über gesamte IT-Landschaft

# Was sich ändern muss

## Was moderne Security heute leisten muss

- Ganzheitlicher Blick auf Endpunkte, Identitäten und Cloud
- Früherkennung statt reiner Reaktion
- Kontinuierliche Überwachung statt punktueller Maßnahmen
- Kombination aus Technologie, Prozessen und Know-how
- Klare Einordnung und strukturierte Reaktion auf Vorfälle



SOFT-CONSULT

# Ganzheitliche Security inkl. Cloud

# Moderne Security bedeutet ganzheitlicher Schutz

- **Zentrale Sicht** auf alle sicherheitsrelevanten Ereignisse
- Verknüpfung von Daten, Zugriffen und Aktivitäten (Verrechtung/Berechtigungen, Data Governance)
- Konsistente Sicherheitsrichtlinien über alle Bereiche hinweg
- Grundlage für effektive Detection & Response
- KI-Nutzung: Wer sieht was? / Zugriff auf was?

SOFT-CONSULT

# Managed Security Service

# Was ist Managed Security?

## Managed Security: Sicherheit als kontinuierlicher Service

- Kontinuierliche Überwachung der gesamten IT-Umgebung
- Früherkennung und Bewertung von Sicherheitsereignissen
- Klare Reaktionsprozesse im Ernstfall
- Transparenz durch regelmäßiges Reporting
- Kombination aus Technologie, Prozessen und Experten-Know-how

# Was ist Managed Security?

**Managed Security:**

Ganzheitlicher Blick auf Ihre Security-Herausforderungen

Aktives Steuern der notwendigen Aufgaben

# Was ist Managed Security?

## Einfache Grundlagen

M365, Cloud-Infrastruktur und Entra ID, Purview sind die Basis für vernünftiges, ganzheitliches Konzept

## Wissen,

welche KI wird im Unternehmen benutzt wird!

## Erweiterung mit XDR

cynet

SOFT-CONSULT

# Exzellenz bestätigt:

## Cynet führt im aktuellen MITRE ATT&CK® Evaluierungsumfeld

# Wofür steht der MITRE ATT&CK® Report

## Der MITRE ATT&CK® Report

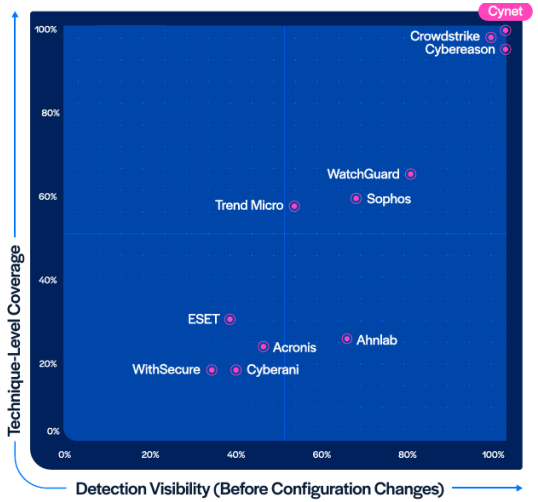
- Unabhängige Evaluierung realer Angriffsszenarien
- Fokus: Detection & Response-Fähigkeiten moderner Security-Lösungen
- Cynet zeigt hohe Erkennungsrate und Transparenz in Angriffsszenarien
- Starke Kombination aus Detection, Analyse und Response

# Unsere Lösung: cynet

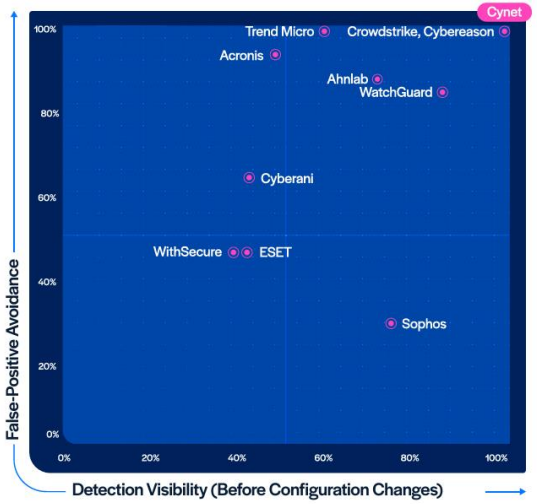
## Nr. 1 im MITRE ATT&CK® Report 2023,2024,2025

- 100% Visibility & 100% Analytic Coverage
- 100% Detection vs. False Positive
- 0 Konfigurationsäderungen
- 0 Fehlalarme

**100% Visibility & 100% Analytic Coverage**




**Detection vs. False Positive**

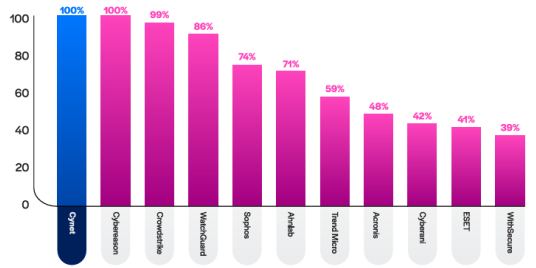


# Unsere Lösung: cynet

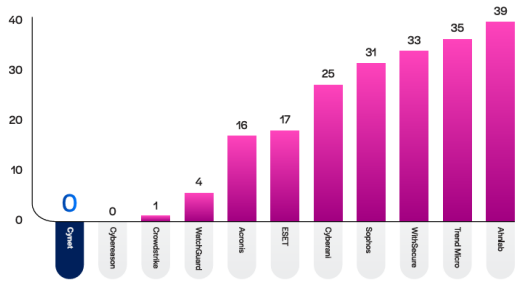
## Nr. 1 im MITRE ATT&CK® Report 2023,2024,2025

- 100% Visibility & 100% Analytic Coverage
- 100% Prevetion Rate bei
- 0 Konfigurationsäderungen
- 0 Fehlalarme

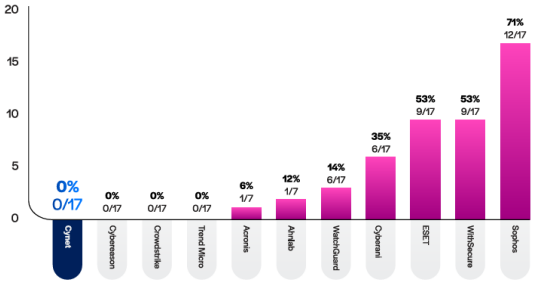
### 100% Sichtbarkeit




### 0 Konfigurationsänderungen




### 0 Fehlalarme



# Was jetzt?

## Managed Security: Was bedeutet das für Sie?

**Automatisierte Threat Detection & Response**:

- Überwachung sicherheitsrelevanter Ereignisse
- Bewertung von Ereignissen **innerhalb von 2 Stunden** (Geschäftszeiten 8–17 Uhr)
- Prüfung / Bearbeitung **innerhalb von 12 Stunden**

**Außerhalb der Geschäftszeiten:**

**Isolation oder Blockierung betroffener Systeme** durch CyOps-Abweichungen (z. B. Wartungen) werden **vorab abgestimmt**

# Business Value

## Mehrwert durch Managed Security

- Frühzeitige Erkennung von Risiken und Angriffen
- Reduzierung von Ausfallzeiten und Schäden
- Entlastung der internen IT
- Klare Transparenz statt „Blackbox Security“
- Grundlage für Compliance (z. B. NIS2)

# Key Take Away!

# Was bringt das eigentlich?

- Schatten-KI erkennen und verhindern
- **Ihre Sicherheit, ihre Prozesse immer im Blick**
- Rechtevergabe/ bessere Userverwaltung: Wer hat auf was Zugriff
- Anomalien rechtzeitig erkennen
- Wichtig: Klassische Endpoint-Security reicht heute nicht mehr aus!

# Keine Angst vor KI wenn Sicherheit gleich mitgedacht wird !

# Vielen Dank!

## Nicht verzagen, Peter fragen!


Peter Janssen

Business Development Representative

Tel. 07345 9611-34

E-Mail peter.janssen@soft-consult.net

SOFT-CONSULT

# Q&A

SOFT-CONSULT

Wir beraten den Mittelstand.

Für digitale Lösungen mit Mehrwert.

Ihr Digitalisierungspartner

**SOFT-CONSULT Häge GmbH**
**Riedheimerstraße 5**
**89129 Langenau**

**07345 9611-0**
**sc@soft-consult.net**
**www.soft-consult.net**