

Informationstag "IT-Forensik"

Berlin, 12.05.2016

IT-Forensik und effiziente Datenanalytik

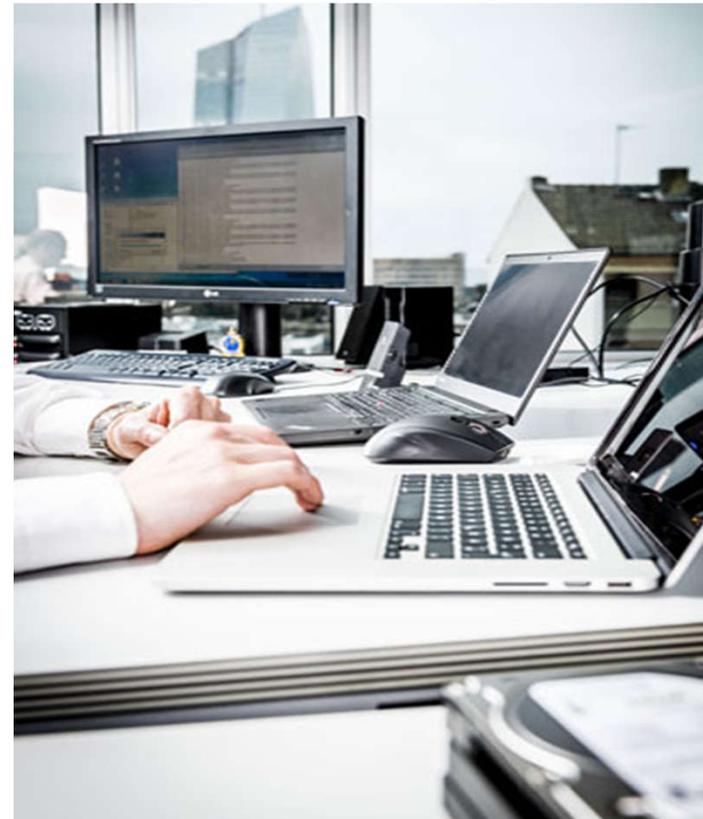
Digitale Spurensuche in Fällen von Wirtschaftskriminalität

Wulf Kollmann

CONTURN Analytical Intelligence Group GmbH

Wer steht vor Ihnen?

- Wulf Kollmann
- Diplom-Informatiker,
Nebenfach Betriebswirtschaft
- IT-Beratung in Konzernen,
Software-Entwicklung und Business
Intelligence
- Seit 2011 bei Conturn Analytical
Intelligence Group GmbH
- Head of Forensic Services &
Project Management



Wirtschaftskriminalität

- Betrug, Korruption, Steuerstraftaten, Insiderhandel, Industriespionage...
- Einige Beispiele sind bekannt aus den Medien
- Viele andere Fälle werden nicht publik (gemacht)



Bevor Strafverfolgungsbehörden einschreiten...

- Interne Ermittlung!
- Interne oder externe Hinweise auf Fehlverhalten
- Informieren der Verantwortlichen z.B. GF
- Einsetzen eines Komitees zur Klärung, ob und wie reagiert werden muss
 - Was ist passiert?
 - Welcher Schaden ist möglicherweise entstanden?
 - Haftungsfrage?
 - Klärung rechtlicher Fragen



Ziele der internen Ermittlung

- Aufklärung des Sachverhalts
- schnell und umfassend
- rechtlich abgesichert
- Sammlung der Beweismittel forensisch korrekt
- gut dokumentiert
- Dabei Einschalten von externem Personal häufig sinnvoll
 - Erfahrung bei der Durchführung von Ermittlungen
 - IT-technisches Wissen und Equipment zu Forensik und Auswertung
 - Neutral und unabhängig

Was wird IT-seitig untersucht?

- Kommunikationsdaten
- Datei-Interaktionen
- Surf-Profil
- Geo-Daten
- Spezielle Dateien (Fall-abhängig)
- Strukturierte Daten



Vorgehensweise

- Aufklärung der IT-Infrastruktur
- Forensische Datenakquise
- Datenerschließung
- Ggf. Datenabschichtung:
Einschränkung auf relevante Daten
- Analyse
- Dokumentation in allen Schritten
- Erstellung eines Abschlussberichts je nach Anforderung



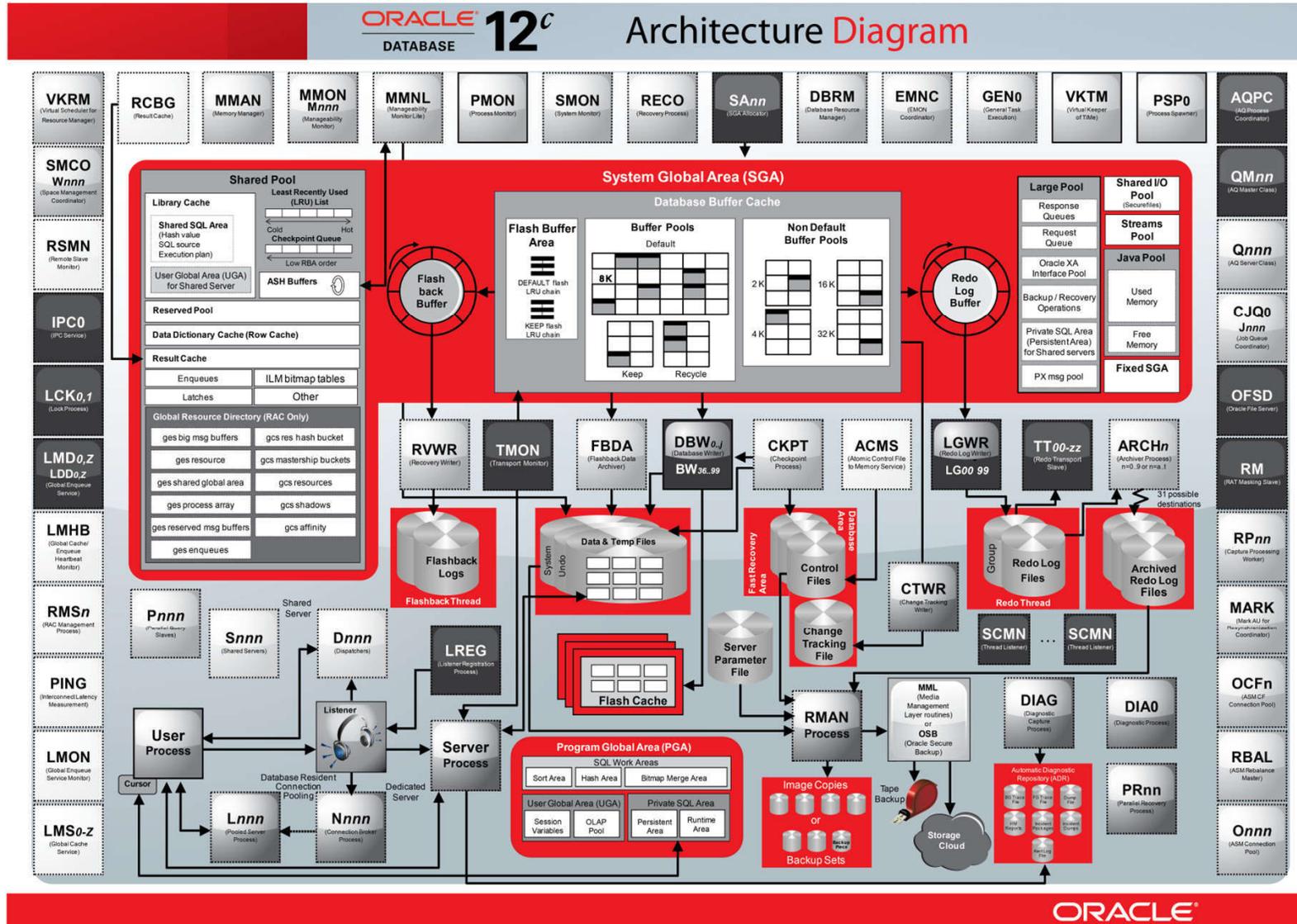
Die grundsätzliche Herausforderung bei der Datenanalyse

- Akquise der Daten aus unterschiedlichsten Quellen
- Komplexität der Daten
- Häufig sehr große Datenmengen, Tendenz steigend

1 Zettabyte (ZB) =	10^{21} Byte = 1 000 000 000 000 000 000 000 Byte (d.h. eine Milliarde Terabyte)
---------------------------	--

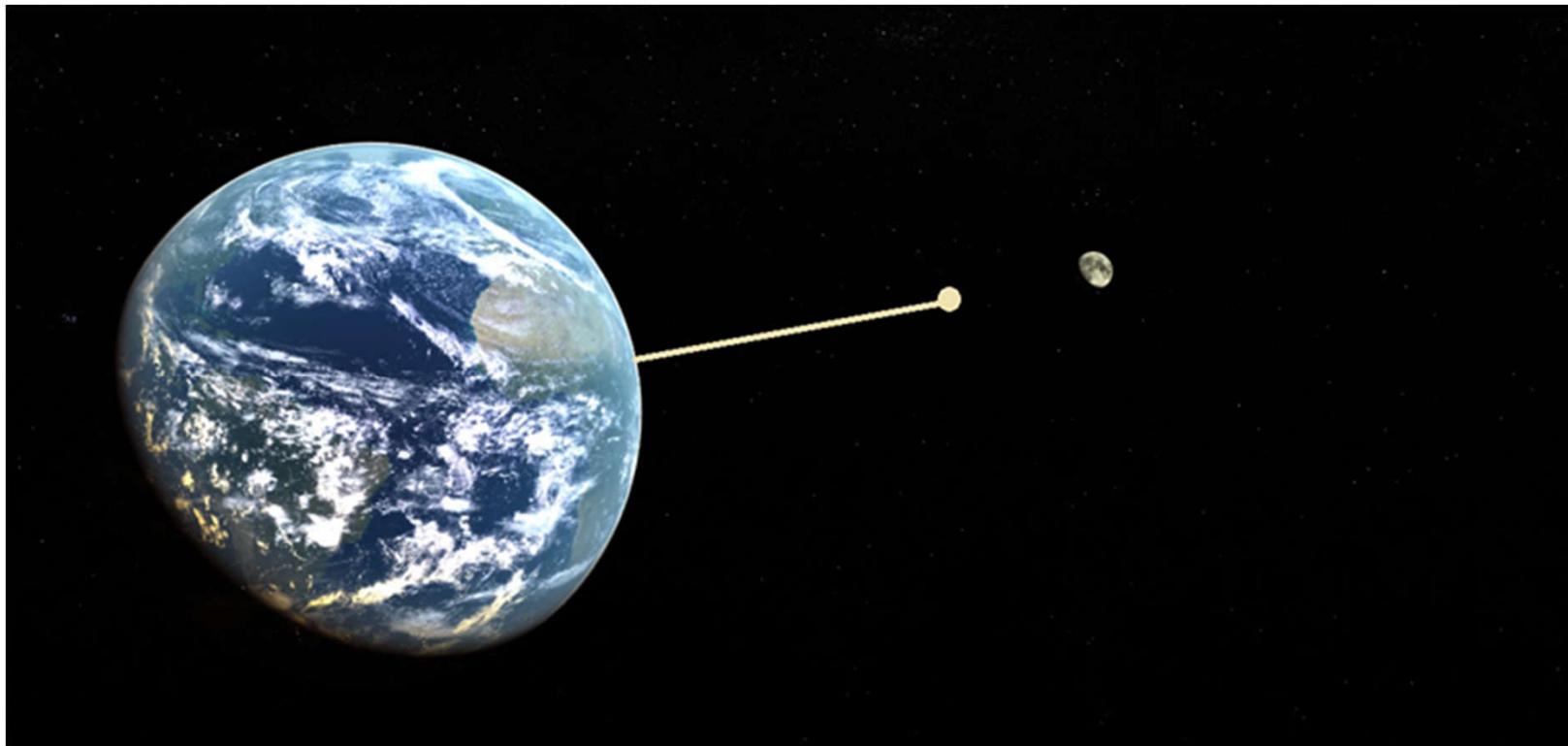
- ... aber meist nicht unbegrenzte Zeit, diese auszuwerten

... Komplexität



... Datenmenge

- Datenzuwachs in 2015: 40 Exabyte (1 Million Terrabyte)



Kleine Datenmenge

Untersuchung im Dienstleistungssektor

- Datenmitnahme
- Ein Verdächtiger
- IT-Geräte:
 - 1 Laptop
 - 1 Smartphone



Mittlere Datenmenge

Untersuchung im Handel

- Betrugsvorwurf
- 1 Hauptverdächtiger
- Mehrere Durchsuchungsobjekte (Büro, Lager, Privatwohnungen)
- Ca. 20 IT-Geräte



Große Datenmenge

Untersuchung im Immobilienumfeld

- Korruptionsverdacht
- mehrere Verdächtige
- Durchsuchung vieler Büros
- Mehrere hundert IT-Geräte sowie Datenbereitstellungen der Firmen



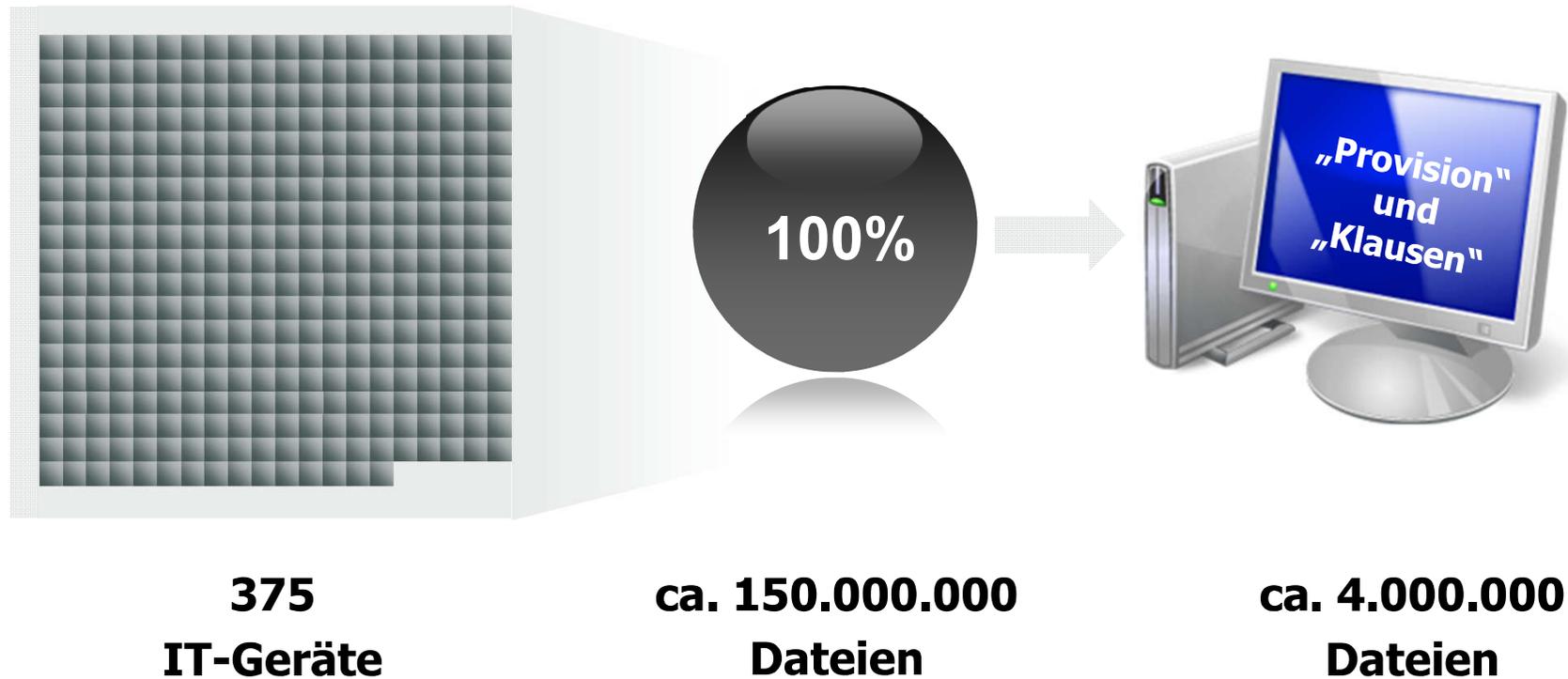
Der (herkömmliche) lineare Ansatz

- Aufbereitung von allen gesicherten IT-Daten
- Suchwortliste erstellen
- Schlagwortsuche und ggf. Extraktion, um Datenvolumen zu reduzieren
- Durchsicht entweder vollständig oder gefiltert nach weiteren Suchbegriffen

Der lineare Ansatz

„Gesucht sind **Provisionen** zwischen Herrn Meyer, Baumeister und **Klausen**“

Alle IT-Geräte, Reduktion durch Schlagworte



Ergebnis des linearen Ansatzes

- Alle Daten enthalten
- Lange Aufbereitungszeiten
- Lange Sichtungszeiten
 - Zu viele Treffer
 - Zu wenige Treffer
- Neue Erkenntnisse und nachgelieferte Daten fließen dadurch erst spät ein

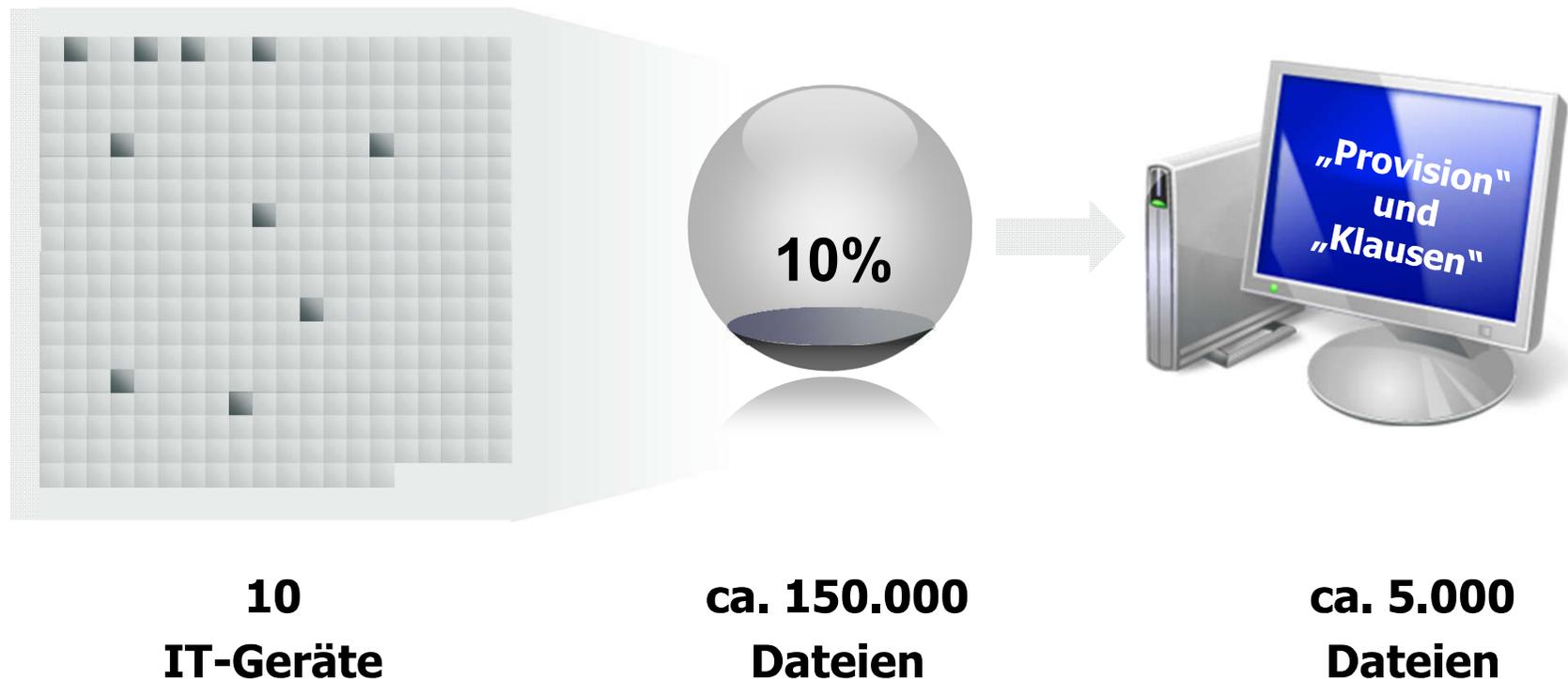
Neue Vorgehensweise

- Start mit den erfolgversprechendsten IT-Geräten und Services
- Ziel: Möglichst schnell Daten zur Sichtung, und dadurch möglichst schnell Erkenntnisse zur weiteren Suche
- Beispiele für neue Erkenntnisse:
 - Verwendete Bezeichnungen bzw. Jargon
 - Weitere Personen involviert
 - Andere E-Mail-Adressen
 - Andere Speicherorte

Der iterative Ansatz: 1. Iteration

„Gesucht sind **Provisionen** zwischen Herrn Meyer, Baumeister und **Klausen**“

Auswahl IT-Geräte, Reduktion durch Schlagworte



Auswahl im Beispiel mittlere Datenmenge

Untersuchung im Handel

- Wirtschaftskriminalität
- 1 Hauptverdächtiger
- Mehrere Durchsuchungsobjekte (Büro, Lager, Privatwohnungen)
- Ca. 20 IT-Geräte



Auswahl im Beispiel große Datenmenge

Untersuchung im Immobilienumfeld

- Wirtschaftskriminalität
- Korruption
- mehrere Verdächtige
- Durchsuchung vieler Büros
- Mehrere hundert IT-Geräte sowie Datenbereitstellungen der Firmen



Vorteile Iterativer Prozess

- Flexibel
- Effektiv, ausgerichtet auf schnellen Erkenntnisgewinn
- Effizient, schnelles Einfließen von neuen Erkenntnissen in die Ermittlung
 - Erkenntnisse aus der vorigen Iteration
 - Erkenntnisse aus anderen Unterlagen
 - Erkenntnisse aus Aussagen und Befragungen
- Parallel arbeitende Teams ermöglichen mehrere Iterationen gleichzeitig

Vielen Dank für Ihre Aufmerksamkeit!

Für weitere Fragen stehen wir Ihnen gerne zu Verfügung:

Wulf Kollmann

Head of Forensic Services & Project Management

E-Mail: wulf.kollmann@conturn.com

Telefon: +49 69 97 99 592-0

Guido Kerbsties

Head of Customer Services

E-Mail: guido.kerbsties@conturn.com

Telefon: +49 69 97 99 592-0

