# Nutzung von Threat Intelligence Sharing Platforms – Ergebnisse einer internationalen Studie

**Daniel Fischer° und Clemens Sauerwein***

° Technische Universität Ilmenau
* Universität Innsbruck

31. DFN-Konferenz „Sicherheit in vernetzten Systemen“
30.-31. Januar 2024, Hamburg

DFN DEUTSCHES FORSCHUNGSNETZ DFN CERT®

# Agenda

- Motivation und Zielsetzung
- Design und Durchführung der Studie
- Ausgewählte Ergebnisse
- Fazit und Ausblick

# Threat Intelligence Sharing Platforms

- unterstützen die Sammlung von Daten aus verschiedenen Quellen, deren Vorverarbeitung und Analyse sowie den Austausch und die Bewertung von Bedrohungs-/Sicherheitsinformationen
- Ziel: Verbesserung der Cyber-Sicherheit durch automatisierte und damit schnellere, zielgenauere und effizientere Erkennung und Bekämpfung von Sicherheitsvorfällen
- Idee/Konzept solcher Plattformen entstand in den frühen 2010er Jahren
  Vgl. Luc Dandurand, Oscar S. Serrano: Towards Improved Cyber Security Information Sharing. In: 5th International Conference on Cyber Conflict (CyCon 2013). Tallinn 2013, S. 1-16.
- heute: breiter und heterogener Markt von TIS-Plattformen
- genauere empirische Erkenntnisse zur Verbreitung und Nutzung dieser fehlen

# Zielsetzung

Wie verbreitet ist der Einsatz von Threat Intelligence Sharing Platforms weltweit?

Wie genau und wofür werden Threat Intelligence Sharing Platforms genutzt?

# Design und Durchführung der Studie

- Bildung von 18 Hypothesen
- Datenerhebung per Online-Fragebogen von April bis Mai 2023
- Grundgesamtheit: Unternehmen, Behörden und Universitäten weltweit
- Aufruf zur Teilnahme per E-Mail und über soziale Medien an CISOs, CIOs und weitere Verantwortliche für Informationssicherheit
- Unterstützer/Multiplikatoren:
  - Forum of Incident Reponse and Security Teams (FIRST)
  - Security Interest Group Switzerland (SIGS)
  - Deutsche Cyber-Sicherheitsorganisation (DCSO) GmbH

# Unsere Stichprobe: 118 Teilnehmende aus 24 Ländern

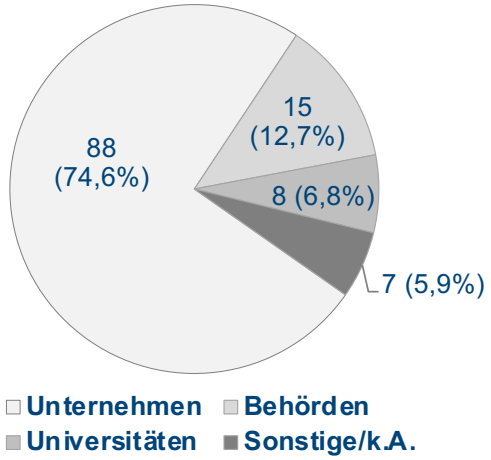
## Geografische Verteilung der Organisationen

| | |
|---|---|
| **Europa** | 76 (64,4%) |
| **Amerika** | 29 (24,6%) |
| **Australien** | 4 (3,4%) |
| **Asien** | 3 (2,5%) |
| **Afrika** | 0 (0%) |

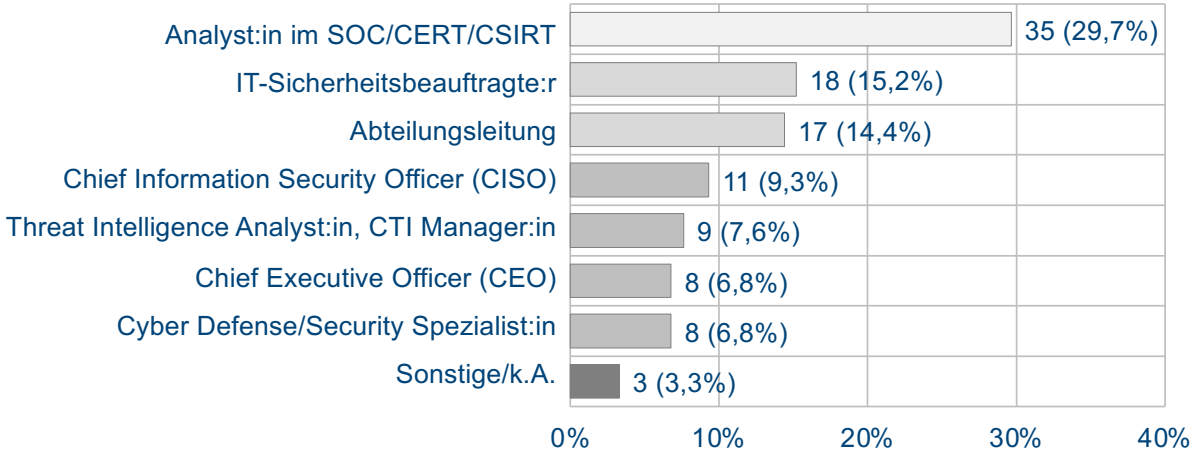
## Größe der Organisationen

| **<50 MA** | **51-500 MA** | **501-5000 MA** | **5001-50000 MA** | **>50000 MA** |
|---|---|---|---|---|
| 18 (25,2%) | 20 (16,9%) | 29 (24,7%) | 24 (20,4%) | 24 (20,3%) |

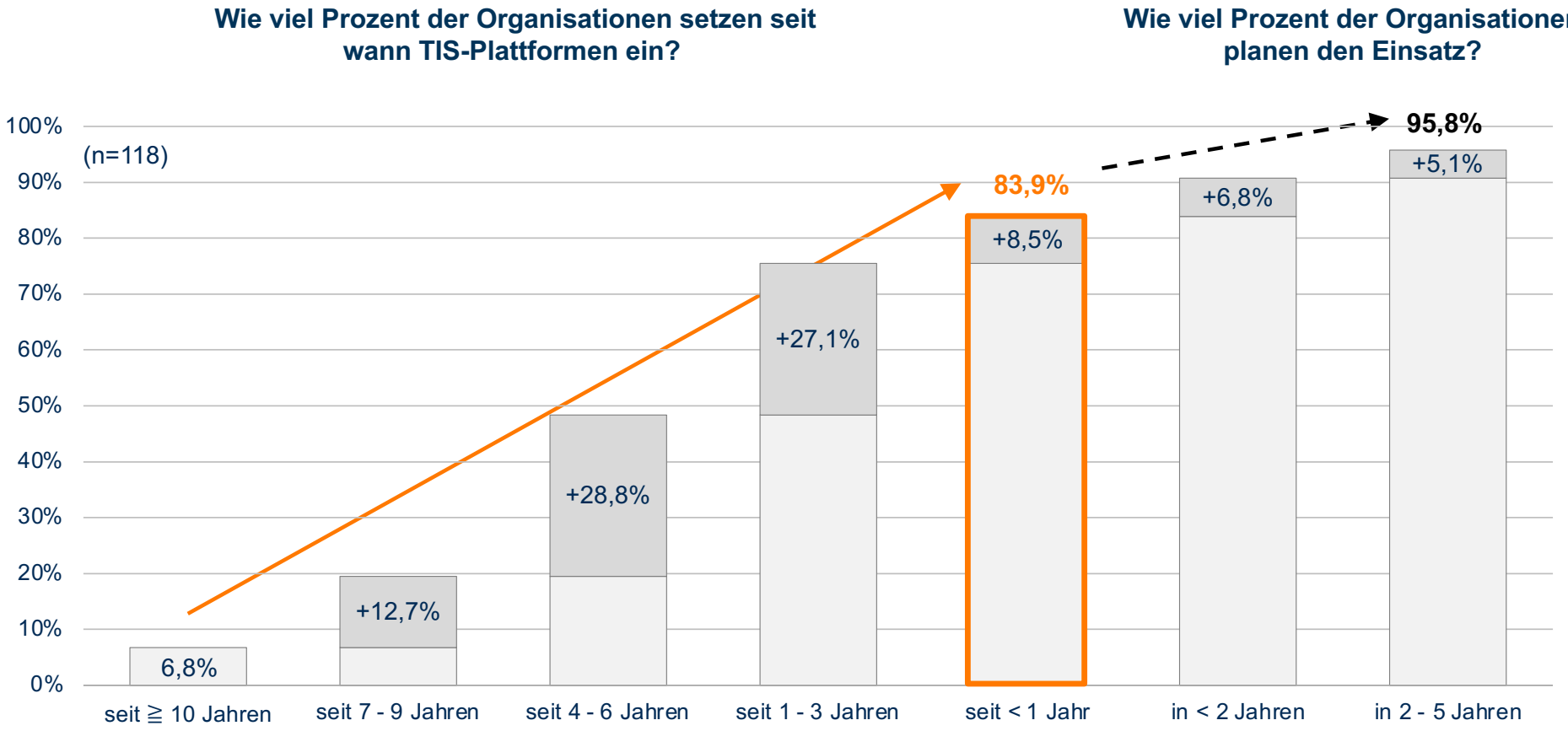
## Art der Organisationen



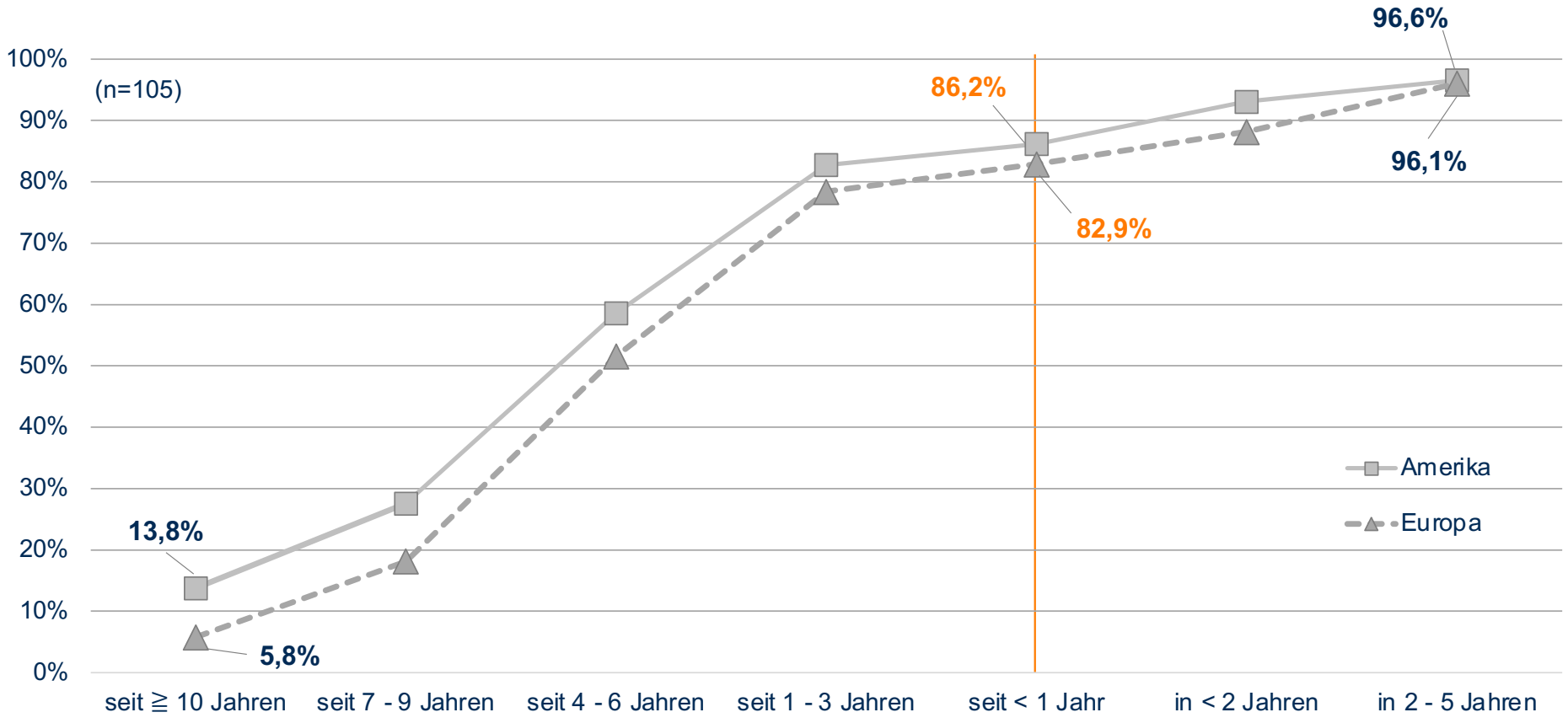

## Rollen der Befragten in der Organisation



# TIS-Plattformen sind weit verbreitet und ihr Einsatz wird zunehmen

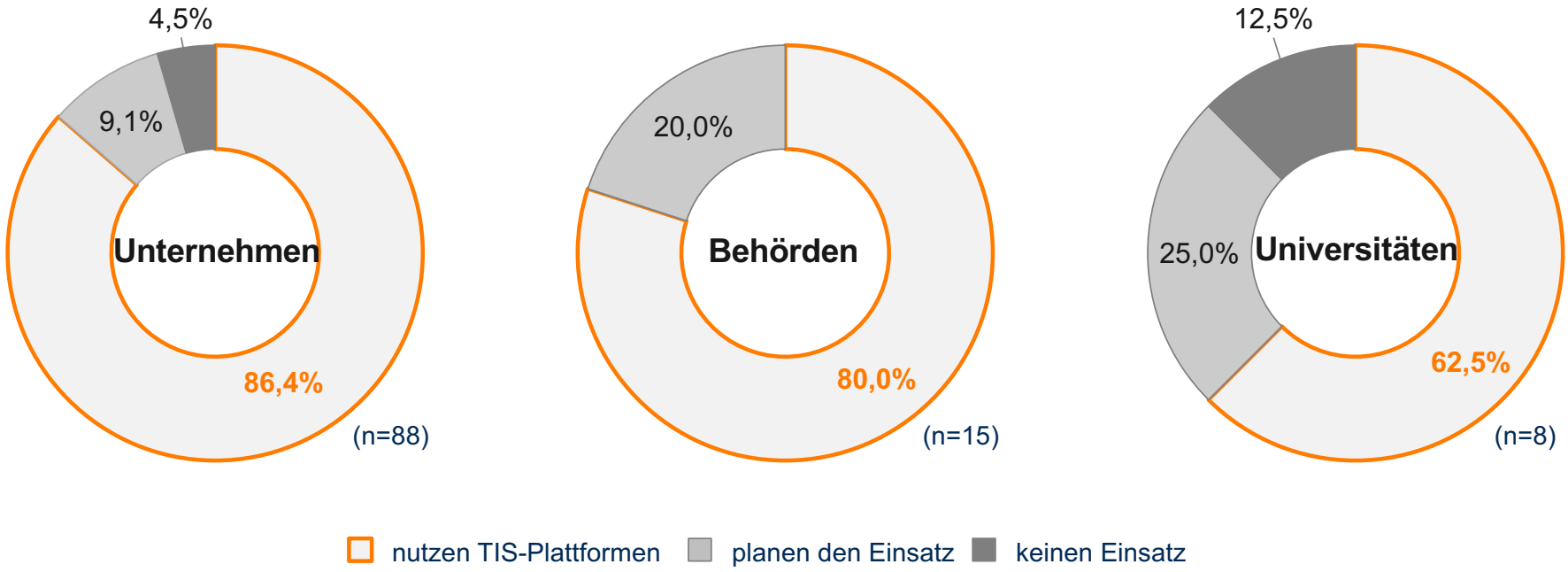


# Einsatz von TIS-Plattformen in Amerika und Europa

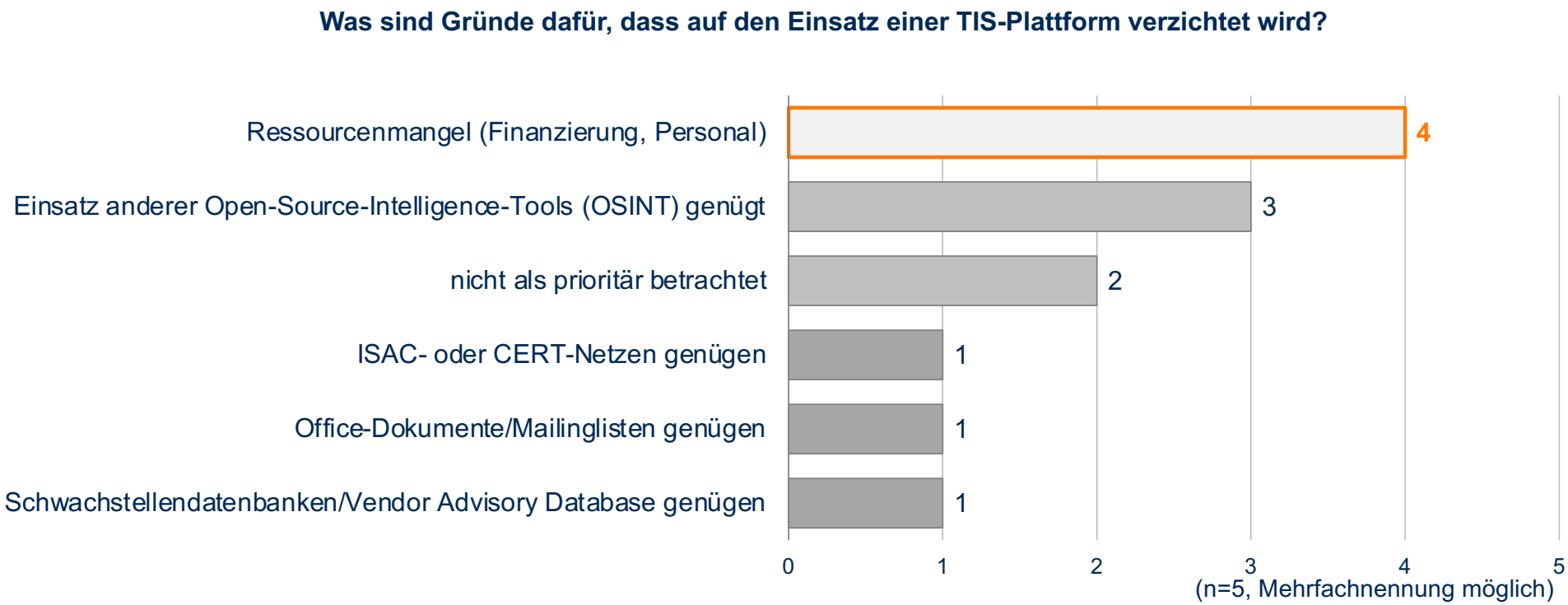


# TIS-Plattformen in Unternehmen am weitesten verbreitet

**Wie viel Prozent der Organisationen setzen TIS-Plattformen ein bzw. planen deren Einsatz?**

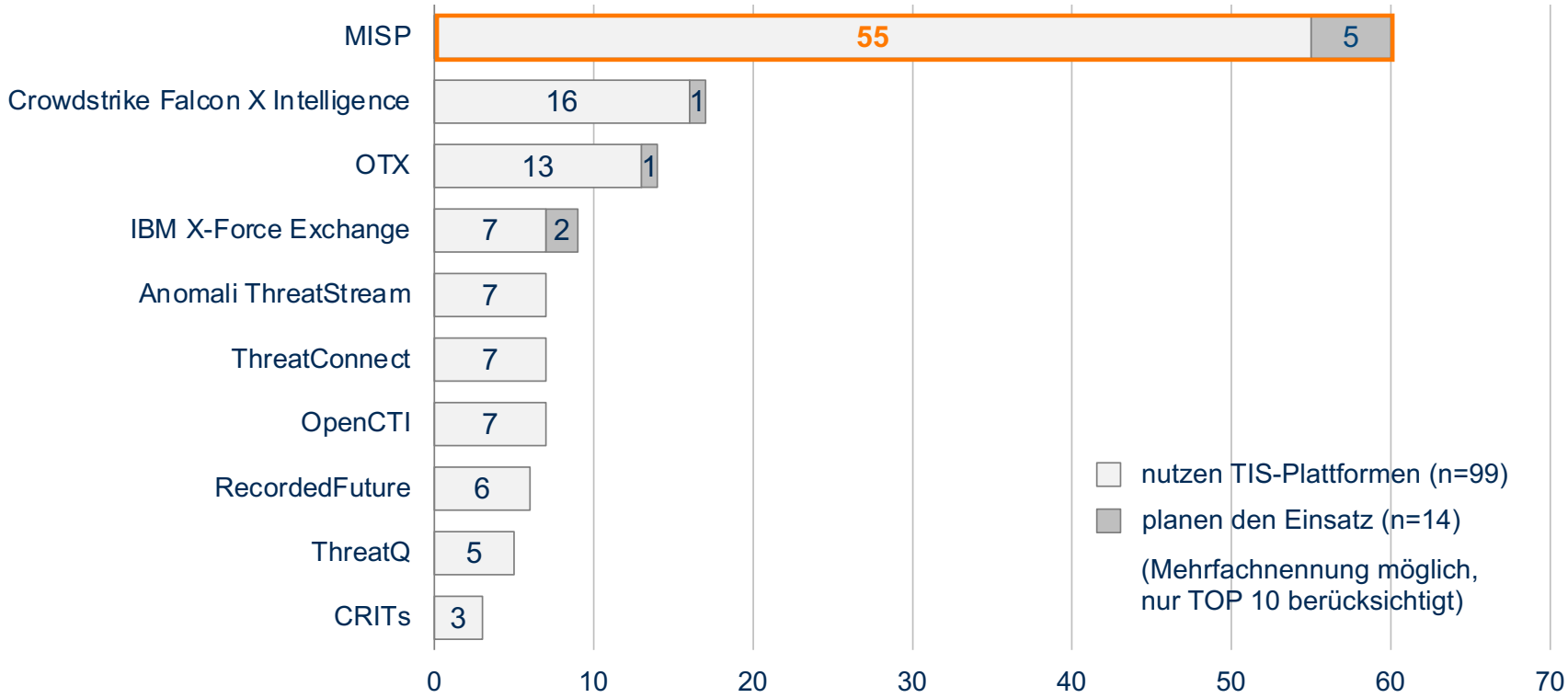


# Verzicht auf TIS-Plattformen aufgrund Ressourcenmangel

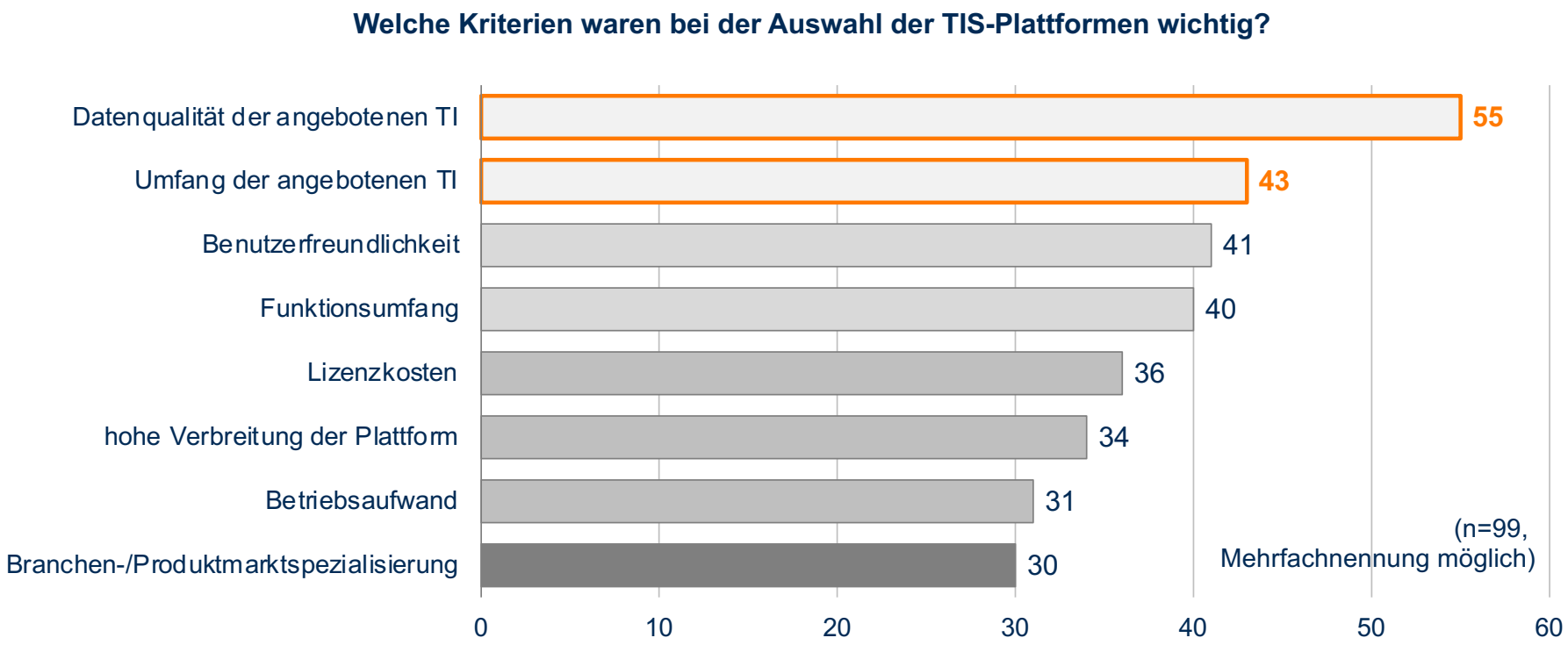


# Malware Information Sharing Platform ist dominierende Plattform

**Welche TIS-Plattform(en) setzen Organisationen ein bzw. planen diese einzusetzen?**

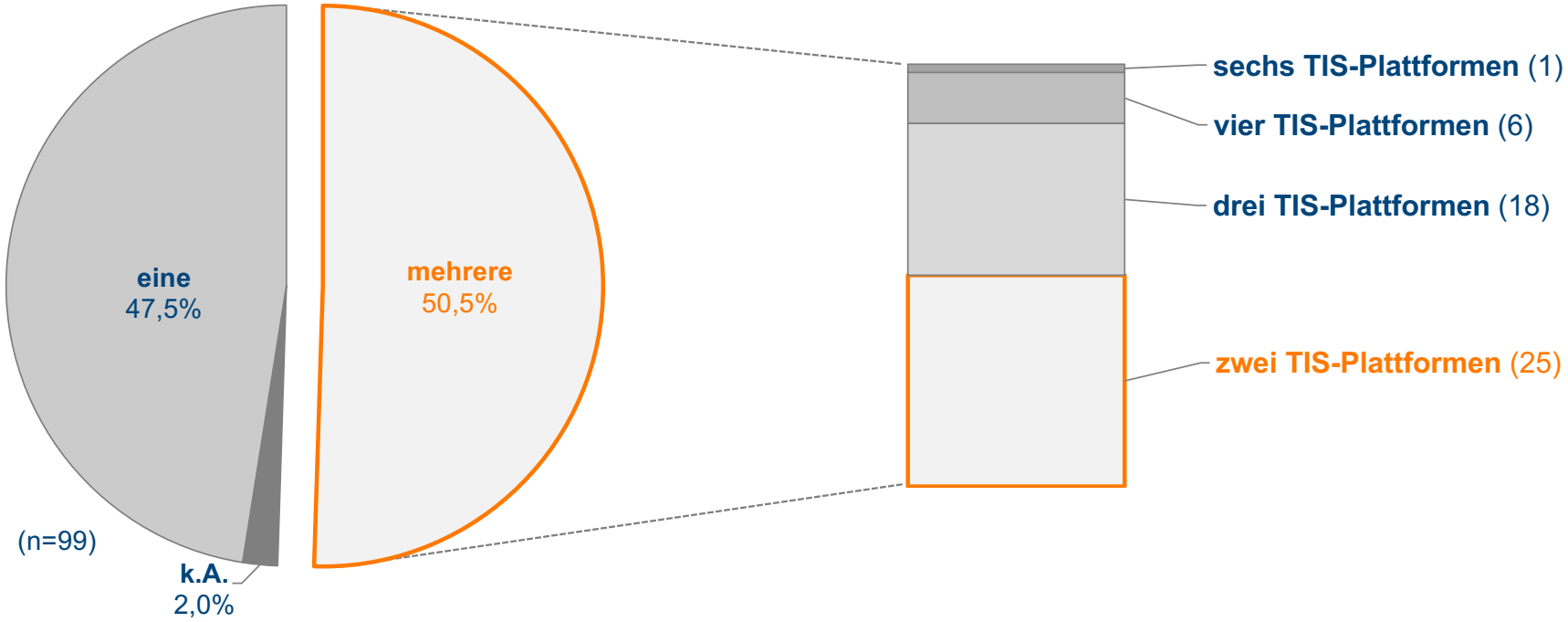


# Qualität und Umfang der TI sind die Hauptkriterien bei der Plattformauswahl

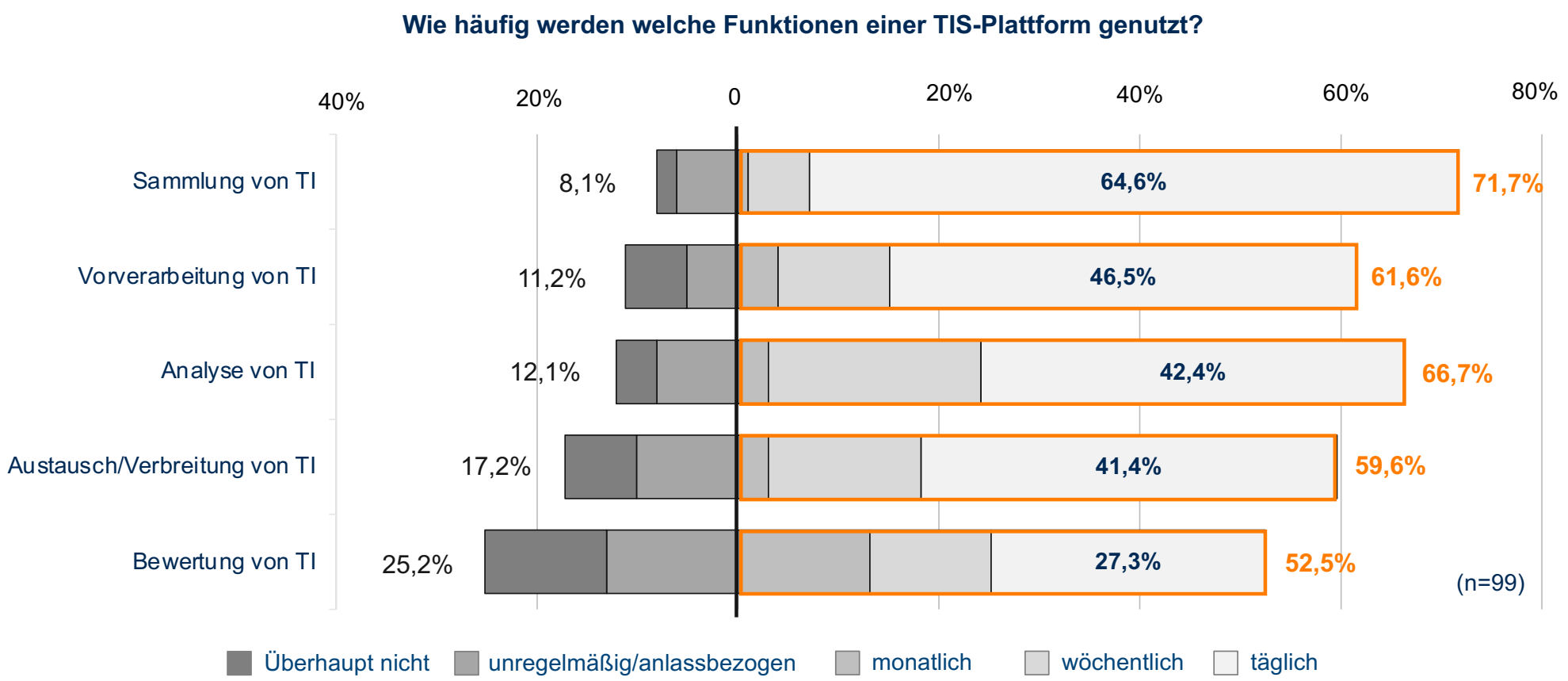


# Gleichzeitige Nutzung mehrerer TIS-Plattformen ist bliebt (zur Kombination deren unterschiedlicher TI und Funktionen)

**Wie viel Prozent der Organisationen nutzen mehrere TIS-Plattformen?**



# TIS-Plattformen werden regelmäßig nicht nur zur Sammlung, Vorverarbeitung, Analyse und Verbreitung, sondern auch zur Bewertung von TI genutzt



# Fazit and Ausblick

- weltweiter Status Quo zur Nutzung von TIS-Plattformen
- nur explorative Resultate (keine Zufallsstichprobe)
- starker Fokus auf Europa und (Nord-)Amerika

- Wiederholung der Studie (Trendanalysen)
- weitere Untersuchungen
  - zu länder- und regionalspezifischen Besonderheiten bei der Nutzung von TIS-Plattformen
  - zum Einsatz von TIS-Plattformen in KMU

# Vielen Dank für Ihre Aufmerksamkeit!

**Dr. Daniel Fischer**

Technische Universität Ilmenau
Group for Information and Knowledge Management

daniel.fischer@tu-ilmenau.de

**Ass.-Prof. Clemens Sauerwein, PhD**

University of Innsbruck
Department of Computer Science

clemens.sauerwein@uibk.ac.at

TECHNISCHE UNIVERSITÄT ILMENAU

universität innsbruck
Institut für Informatik