DACH Threat Intelligence Sharing Platforms Survey 2022

Ausgewählte Ergebnisse einer Studie zur Nutzung von Threat Intelligence Sharing Platforms in Deutschland, Österreich und der Schweiz

Daniel Fischer, Clemens Sauerwein

TECHNISCHE UNIVERSITÄT ILMENAU

universität innsbruck
Institut für Informatik

30. DFN-Konferenz, 08.-10.02.2023, Hamburg

Agenda

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

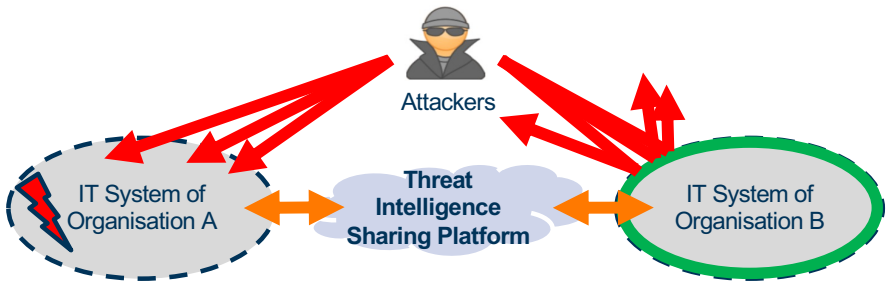
Ausgangspunkt / Motivation

Threat Intelligence Sharing

- (organisationsübergreifender) Austausch von Bedrohungs-/Sicherheitsinformationen
- wichtiger Baustein zur Verbesserung der Cyber-Sicherheit
- Organisationen verfügen dazu oft nicht über ausreichende Ressourcen
- Idee: Automatisierung des TIS

Threat Intelligence Sharing Platforms

- unterstützen die Sammlung von Daten aus verschiedenen Quellen, deren Aggregation und kooperative Auswertung sowie den Austausch von Bedrohungs-/Sicherheitsinformationen
- heute: heterogener Markt von Lösungen
- genauere empirische Erkenntnisse zur Nutzung von TIS-Platforms fehlen



Zielsetzung / Forschungsfragen

Wie verbreitet ist der Einsatz von Threat Intelligence Sharing Platforms im DACH-Raum?

Wie genau und wofür werden Threat Intelligence Sharing Platforms genutzt?

Agenda

- Motivation und Zielsetzung
- **Vorbereitung und Durchführung der Studie**
- Ausgewählte Ergebnisse der Studie
- Fazit und Ausblick

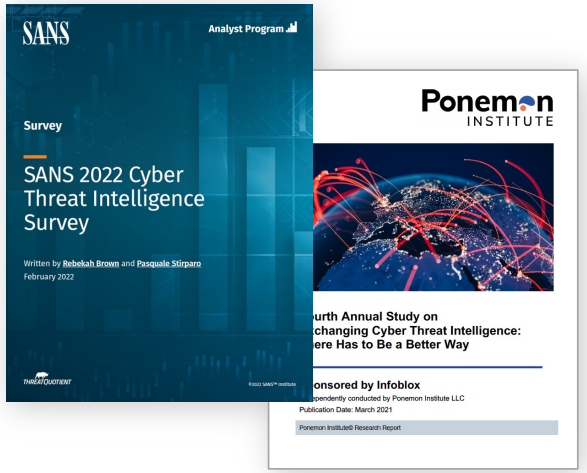
Hypothesenbildung

„Anbietersicht“

- Untersuchung von über 50 TIS-Platforms
- Expertengespräche

„Nutzersicht“

- Auswertung aktueller Studien/Reports
- systematische Literaturanalyse (Fallstudien)



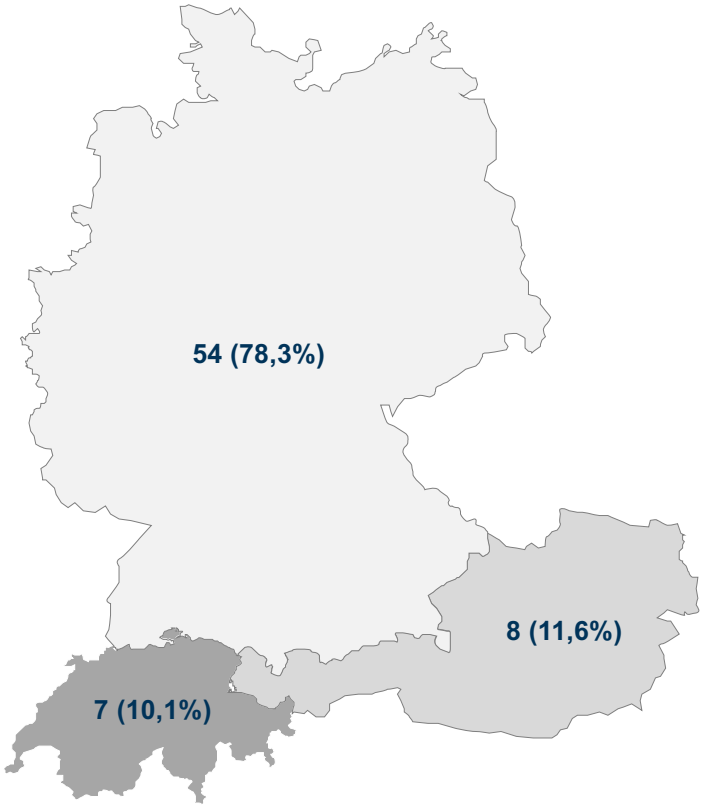
Datenerhebung: Internet-basierte Befragung

- Online-Fragebogen
- Zeitraum: Juli bis September 2022
- Grundgesamtheit: Organisationen in D, A und der CH
  - börsennotierte Unternehmen,
  - Bundesbehörden und
  - öffentliche Universitäten
- Ansprache von CISOs, CIOs und weiteren Verantwortlichen für Informationssicherheit

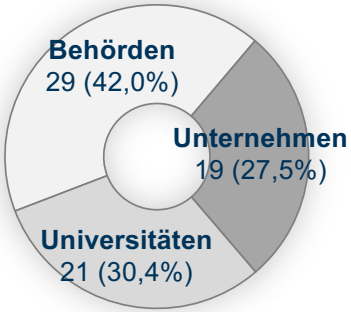
Unternehmen		Universitäten		Behörden	
Deutschland	89	Deutschland	84	Deutschland	92
Österreich	20	Österreich	22	Österreich	15
Schweiz	20	Schweiz	14	Schweiz	24
	129		**120**		**131**

Gesamt	
Deutschland	265
Österreich	57
Schweiz	58
	380

69 Befragungsteilnehmer:innen (Stichprobe)



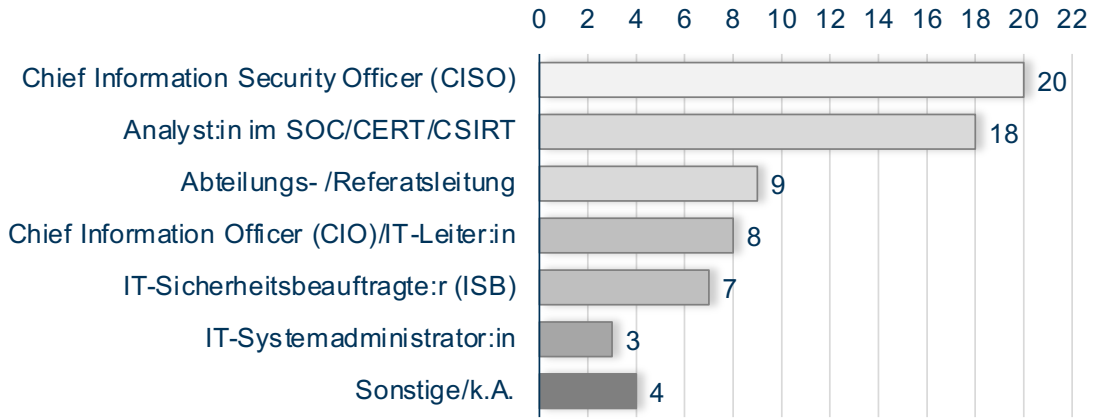
nach Organisationsart



nach Größe

<501 MA	501-5000 MA	5001-50000 MA	>50000 MA
10 (14,5%)	29 (42,0%)	18 (26,1%)	12 (17,4%)

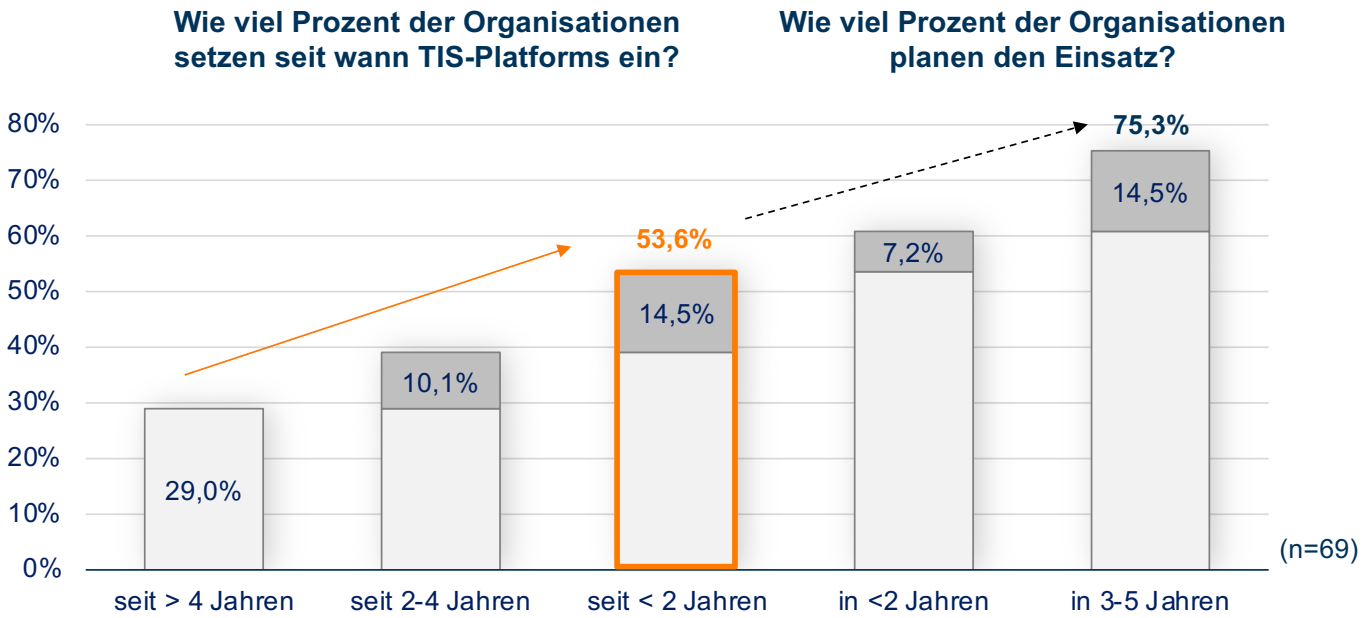
nach Rolle der Befragten



Agenda

- Motivation und Zielsetzung
- Vorbereitung und Durchführung der Studie
- **Ausgewählte Ergebnisse der Studie**
- Fazit und Ausblick

Hypothese 1: Der Einsatz von TIS-Platforms hat in den letzten vier Jahren zugenommen.

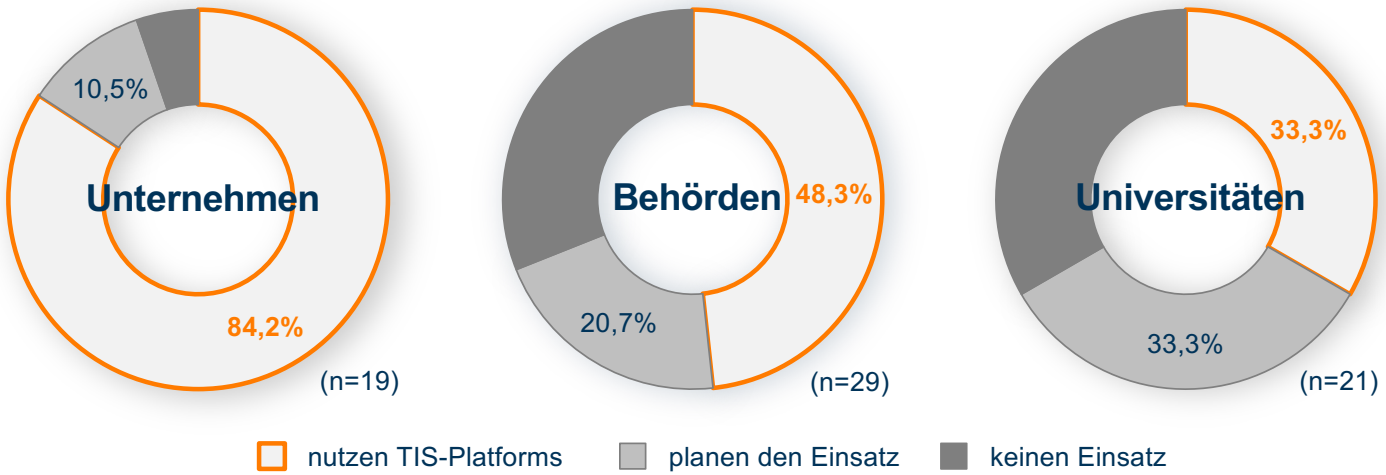


Hypothese bestätigt!

- Threat Intelligence Sharing Platforms sind in der Praxis angekommen!
- Prognose: Einsatz wird noch weiter zunehmen.

Hypothese 2: In Unternehmen ist im Vergleich zu Behörden und Universitäten der Einsatz von TIS-Platforms verbreiteter.

Wie viel Prozent der Organisationen, setzen TIS-Platforms ein bzw. planen deren Einsatz?

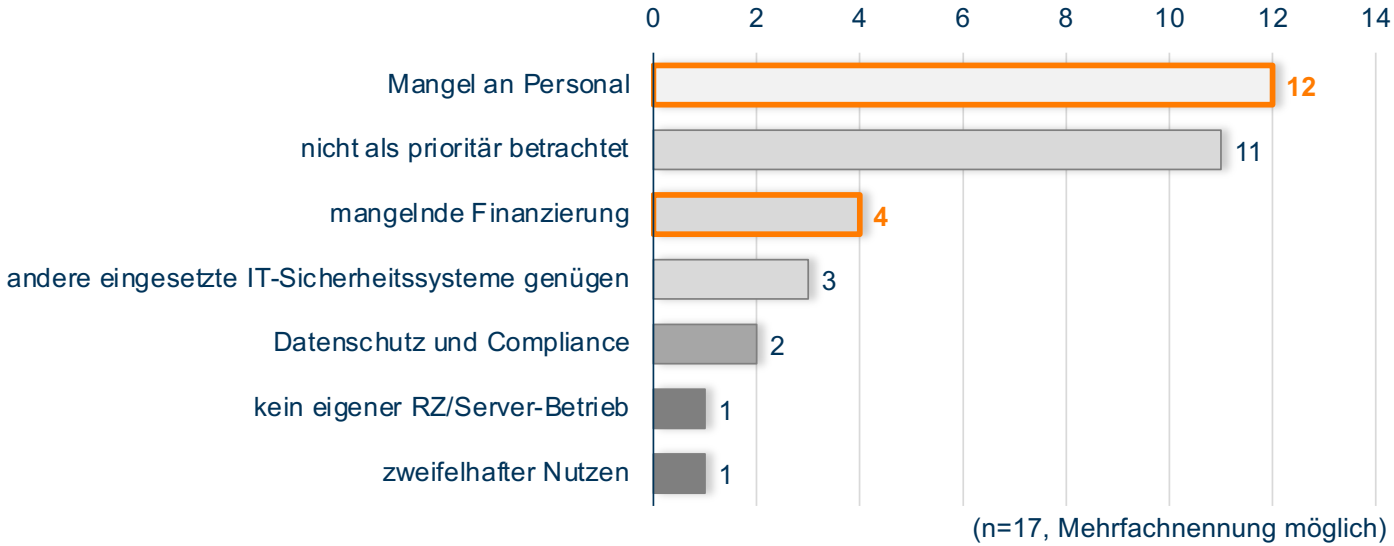


Hypothese bestätigt!

- Einsatz in Unternehmen am weitesten verbreitet
- Behörden und Universitäten wollen aber in den nächsten Jahren aufholen.

Hypothese 3: Die häufigsten Gründe, warum TIS-Platforms nicht eingesetzt werden, sind begrenzte Ressourcen sowie Datenschutz- und Compliance-Bedenken.

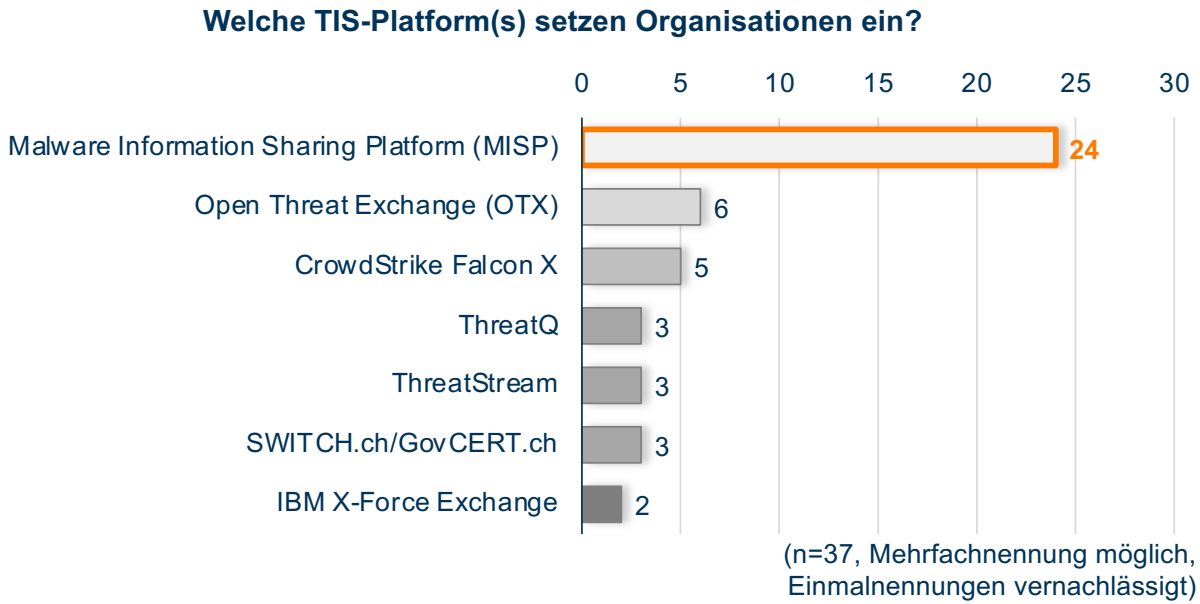
Was sind Gründe dafür, dass auf den Einsatz einer TIS-Platform verzichtet wird?



Hypothese nicht bestätigt!

- Hauptgrund für Nichtnutzung: Ressourcenmangel
- Datenschutz- und Compliance-Bedenken nicht unter den TOP-3-Hemmnissen

Hypothese 4: Trotz des zunehmenden Angebots an TIS-Platforms gibt es eine Konzentration auf einzelne, marktdominierende Plattformen.

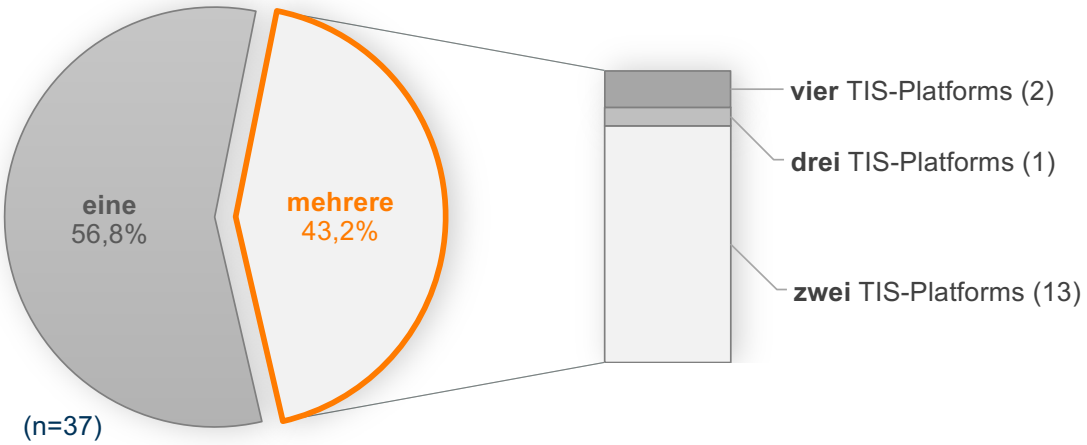


Hypothese bestätigt!

- MISP dominiert!
- Free-to-Use/Open-Source TIS-Platforms verbreiteter als kommerzielle

Hypothese 5: Die gleichzeitige Nutzung mehrerer TIS-Platforms ist eher selten.

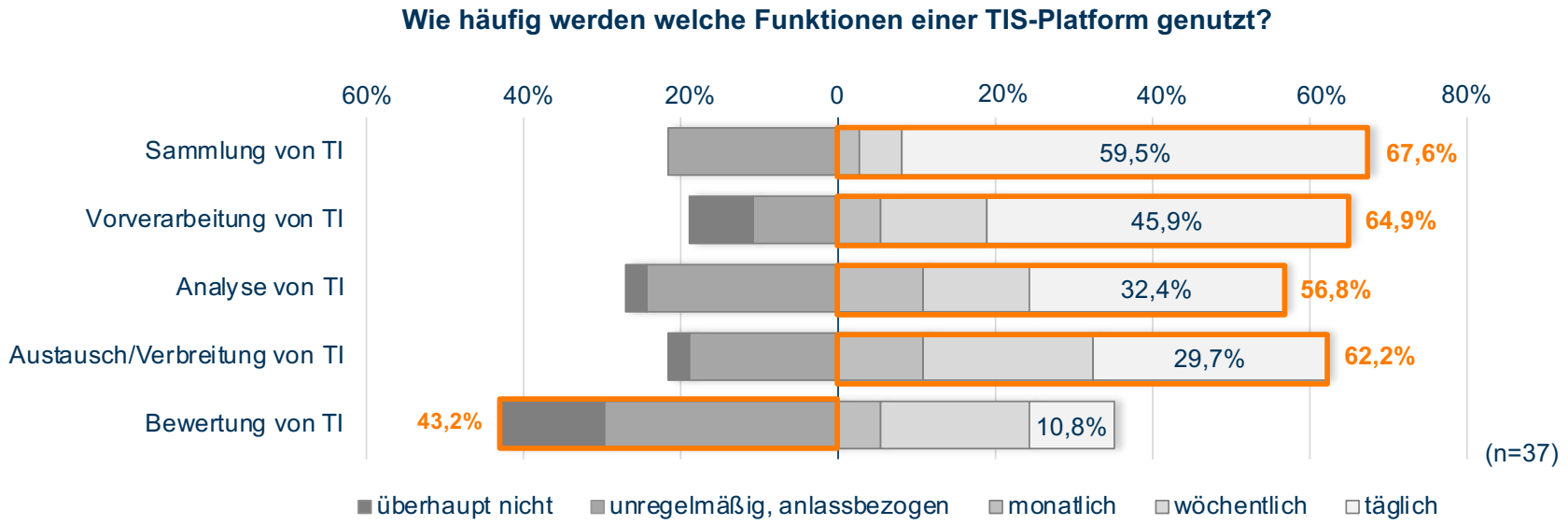
Wie viel Prozent der Organisationen nutzen mehrere TIS-Platforms?



Hypothese nicht bestätigt!

- Fast die Hälfte der Organisationen, die TIS-Platforms nutzen, setzen mehrere gleichzeitig ein.
- beliebte Kombination: Free-to-Use/Open-Source TIS-Platform + kommerzielle TIS-Platform

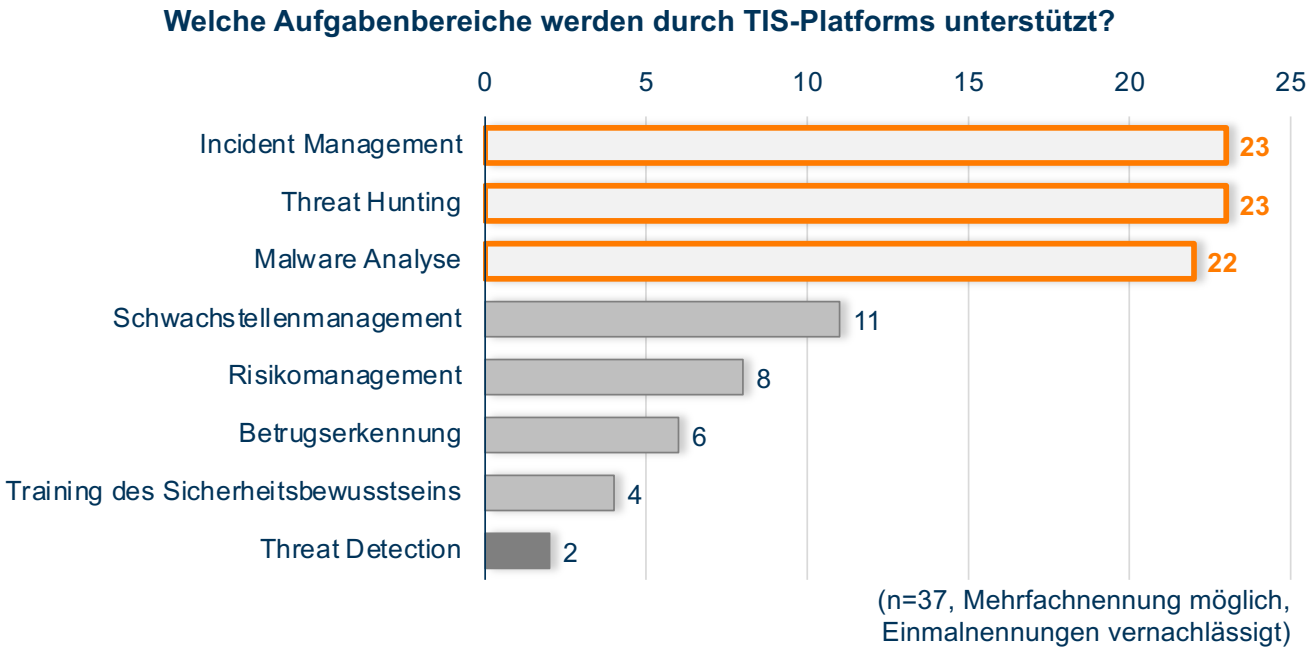
Hypothese 6: TIS-Platforms werden bevorzugt zur Sammlung, Vorverarbeitung und Analyse und weniger zum Austausch und zur Bewertung von TI genutzt.



- Sammlung, Vorverarbeitung, Analyse und Austausch regelmäßig
- Bewertung/Feedback überwiegend unregelmäßig bzw. nicht genutzt

Hypothese nicht bestätigt!

Hypothese 7: Am häufigsten setzen Organisationen TIS-Platforms zur Unterstützung im Aufgabenbereich Incident Management ein.

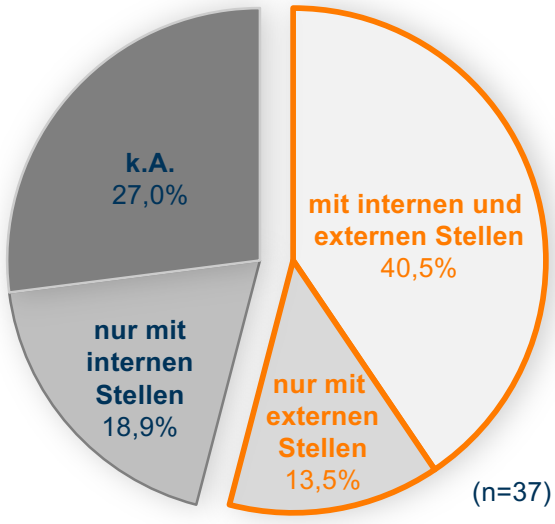


Hypothese bestätigt!

- TOP-3-Einsatzgebiete: Incident Management, Threat Hunting, Malware-Analyse

Hypothese 8: Organisationen teilen Threat Intelligence mithilfe von TIS-Platforms eher nur organisationsintern und nicht organisationsextern.

Mit wem werden Bedrohungsinformationen mithilfe der TIS-Platforms geteilt?



Hypothese nicht bestätigt!

- Mehrheit nutzt TIS-Platforms zum Austausch von Threat Intelligence mit externen Partnern/Stellen

Agenda

- Motivation und Zielsetzung
- Vorbereitung und Durchführung der Studie
- Ausgewählte Ergebnisse der Studie
- **Fazit und Ausblick**

Fazit und Ausblick

- Status Quo der Verbreitung und Aussagen zur Nutzung von TIS-Platforms in D, A und der CH
- explorative Resultate (keine Zufallsstichprobe)
- starker Fokus auf große Organisationen und auf D

- Wiederholung der Studie (Trendanalysen)
- internationale Ausweitung der Studie in Kooperation mit
  - Forum of Incident Response and Security Teams (FIRST),
  - Security Interest Group Switzerland (SIGS),
  - u.a.

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Daniel Fischer
Technische Universität Ilmenau
Fachgebiet Informations- und Wissensmanagement
daniel.fischer@tu-ilmenau.de

Ass.-Prof. Clemens Sauerwein, PhD
Universität Innsbruck
Institut für Informatik
clemens.sauerwein@uibk.ac.at

TECHNISCHE UNIVERSITÄT ILMENAU

universität innsbruck
Institut für Informatik