Insights into the Distribution and Use of Threat Intelligence Sharing Platforms

Clemens Sauerwein* and Daniel Fischer°

* University of Innsbruck (Austria)
° Technische Universität Ilmenau (Germany)

06-03-2024

Security Interest Group Switzerland – 23rd SOC Forum

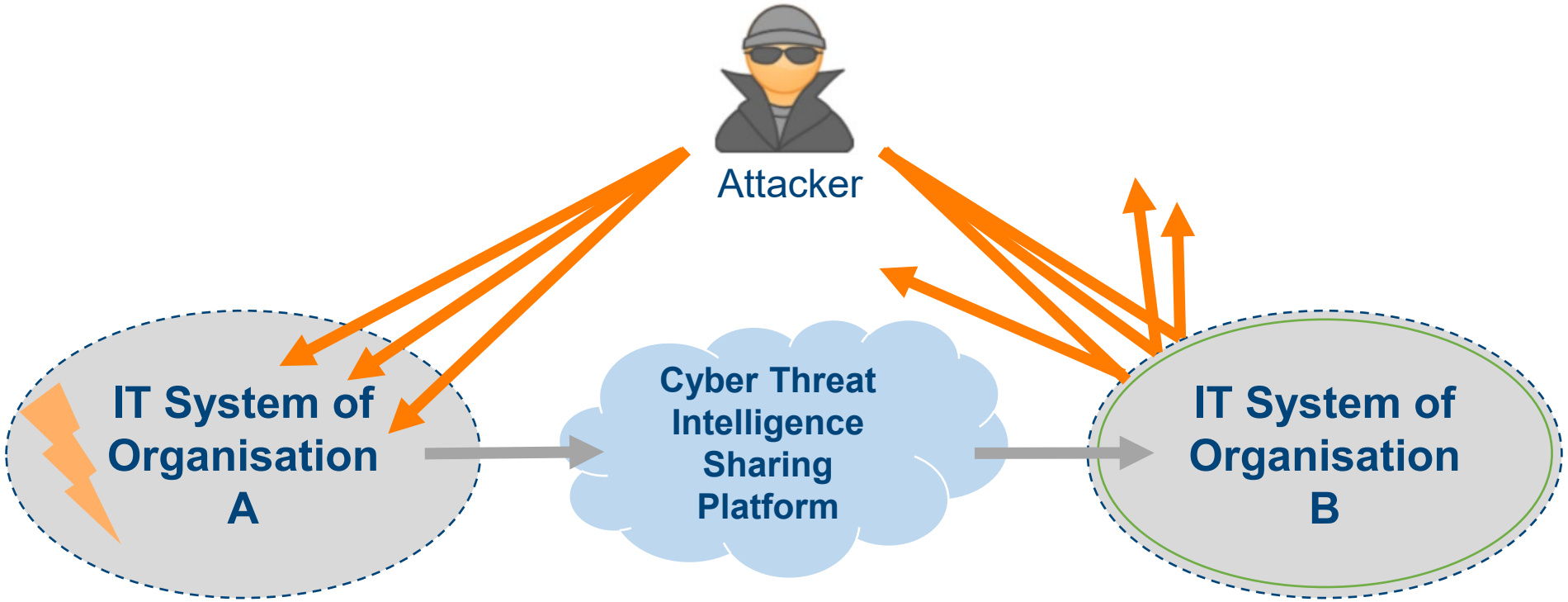
Hilton Zürich Airport, Switzerland

TLP:Green

Agenda

- Motivation
- Study Details
- Key Findings
- Conclusion & Outlook

Motivation



…supports the **collection** of threat data from multiple sources, their **pre-processing** and (joint) **analysis**, as well as the (cross-organizational) **dissemination** and assessment of security information

…more precise empirical findings on the distribution and use of platforms are often lacking

Research Questions

How widespread are threat intelligence sharing platforms?

How exactly and for what are threat intelligence sharing platforms used?

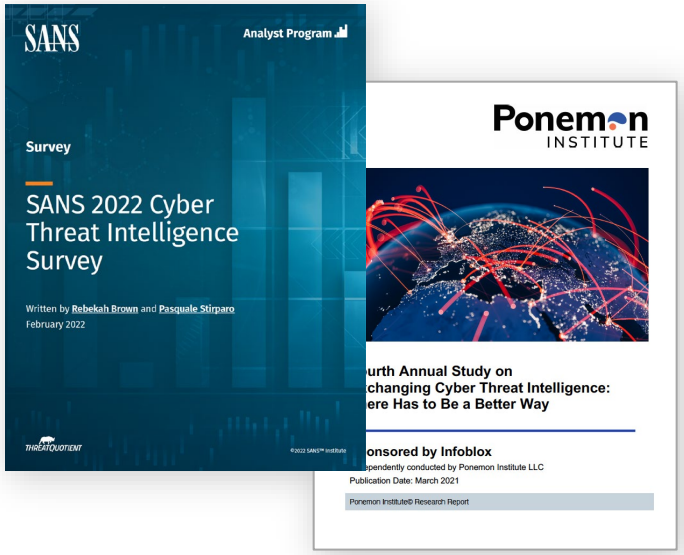
Making Claims About the Use of Threat Intelligence Sharing Platforms

„Provider Perspective“

- investigation of over 50 platforms
- expert interviews

„End-User Perspective“

- evaluation of current studies/reports
- systematic literature analysis (case studies)



Data Collection: Internet-based Survey

- online questionnaire
- survey period: April to May 2023
- population: organizations in America, Europe, Asia, Australia and Africa
  - companies,
  - federal authorities, and
  - public universities
- calls for participation by email and social media to CIOs, CISOs and other security professionals
- our supporter:
  - Forum of Incident Reponse and Security Teams (FIRST)
  - Security Interest Group Switzerland (SIGS)
  - Deutsche Cyber-Sicherheitsorganisation (DCSO) GmbH

Our Sample: 118 Survey Participants From 24 Countries

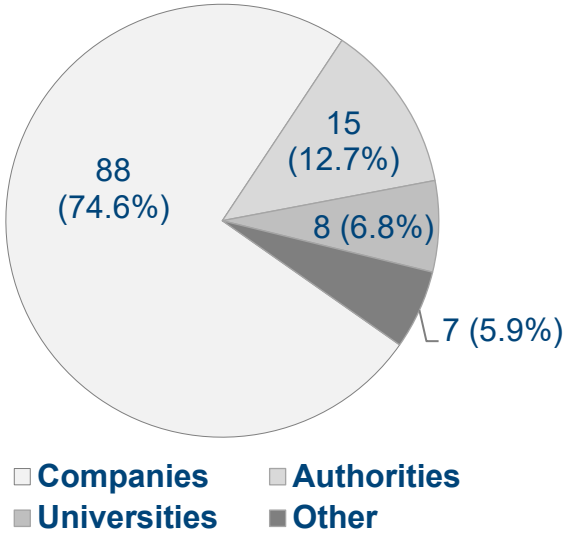
Geographical distribution of organisations

Europe	76 (64.4%)
America	29 (24.6%)
Australia	4 (3.4%)
Asia	3 (2.5%)
Africa	0 (0%)

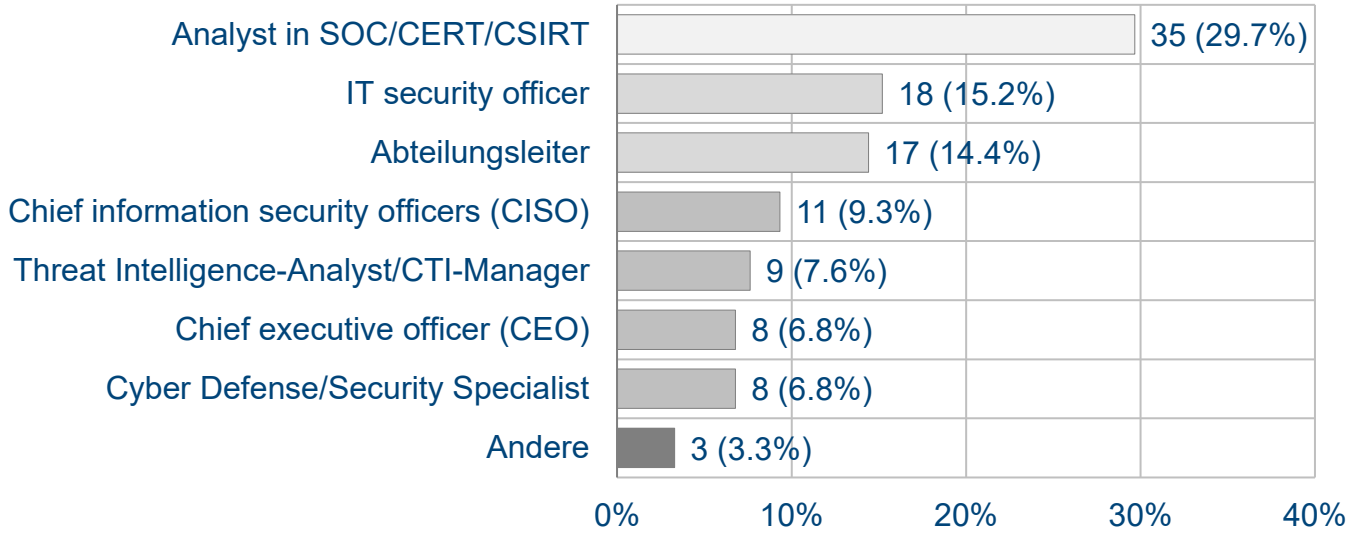
Size of organisations

<50 EMPL	**51-500 EMPL**	**501-5000 EMPL**	**5001-50000 EMPL**	**>50000 EMPL**
18 (25.2%)	20 (16.9%)	29 (24.7%)	24 (20.4%)	24 (20.3%)

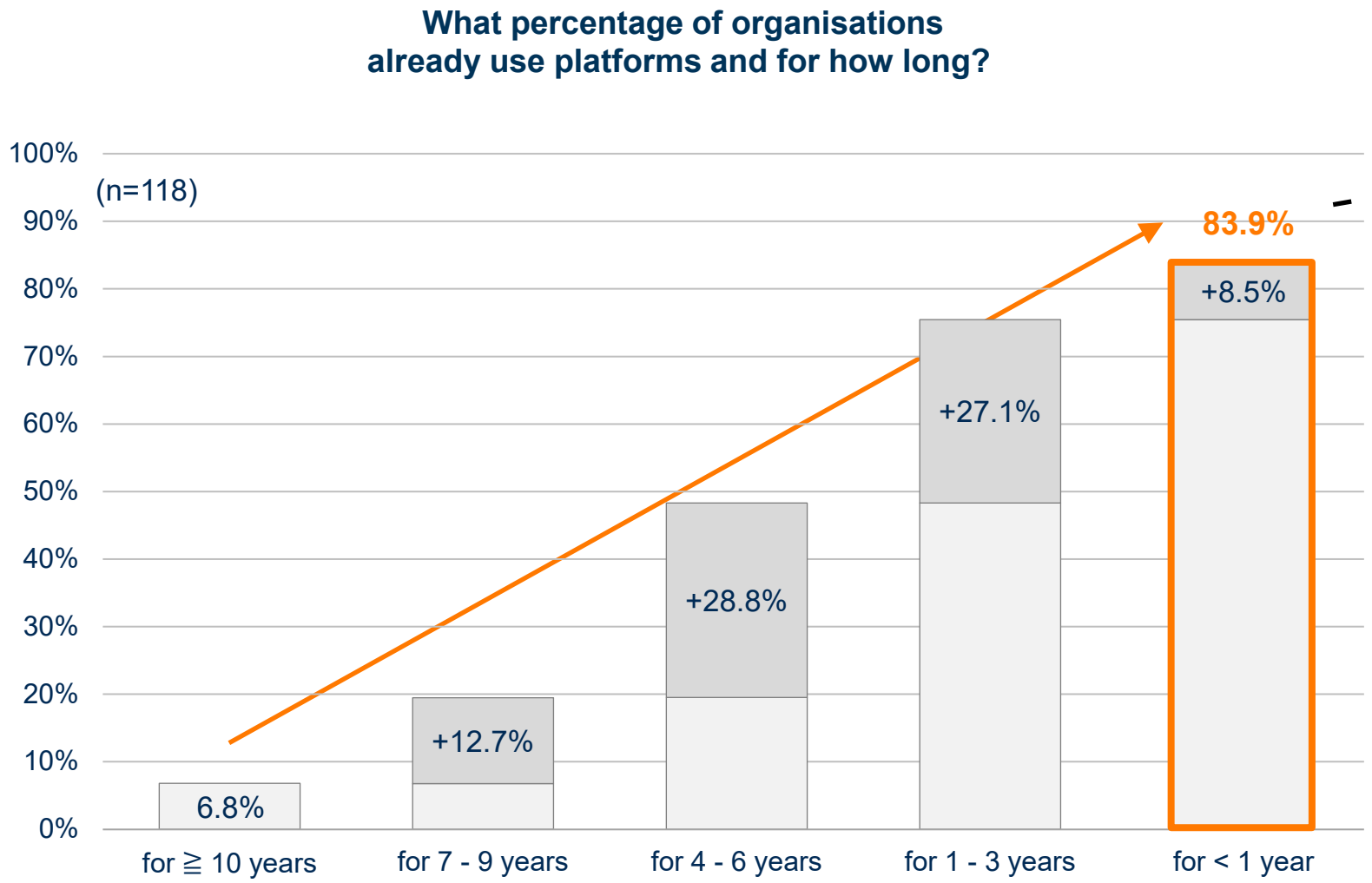
Type of organisations



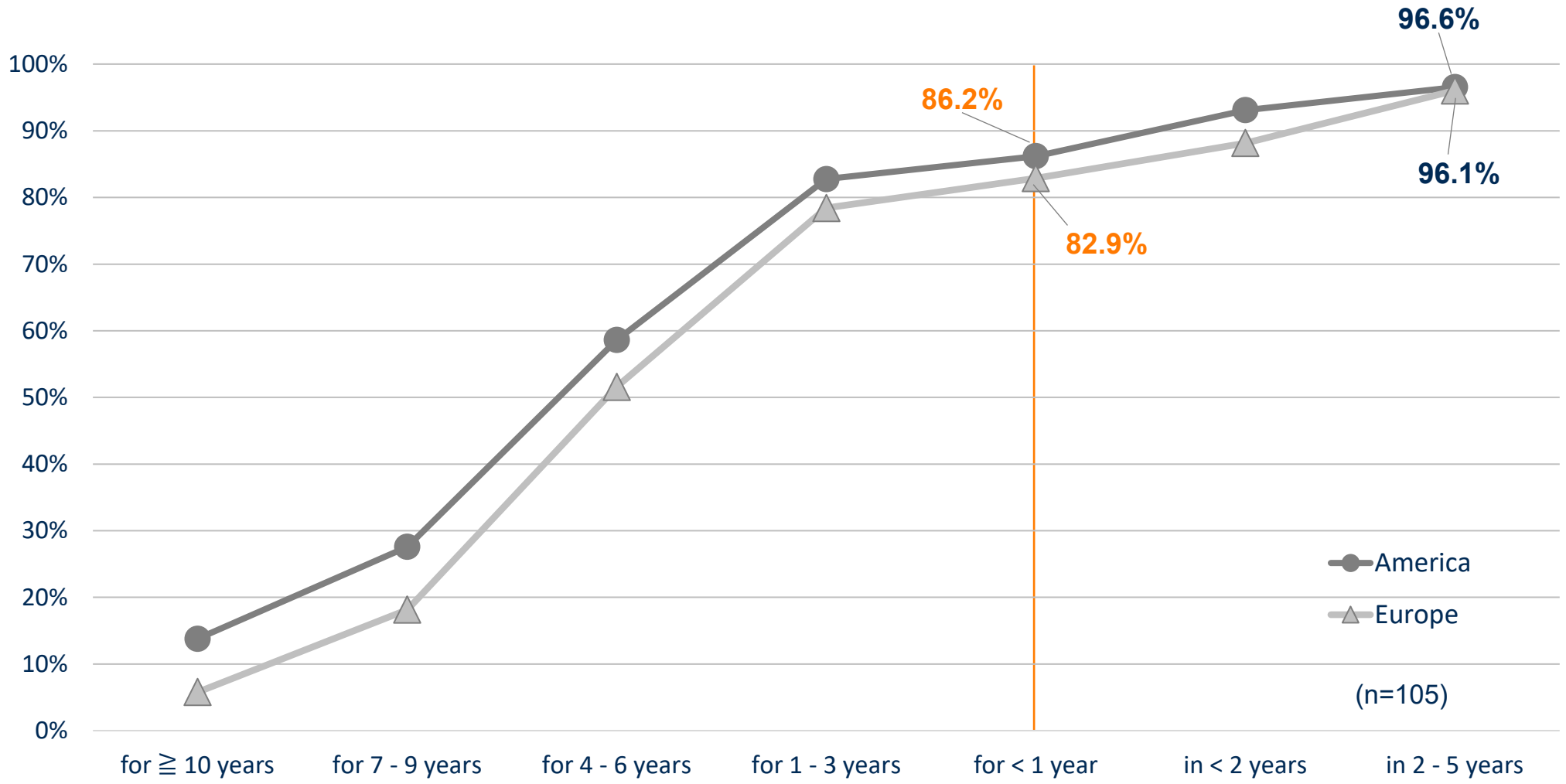
Roles of participants within the organisation



Platforms Are Widespread and Their Use Will Increase

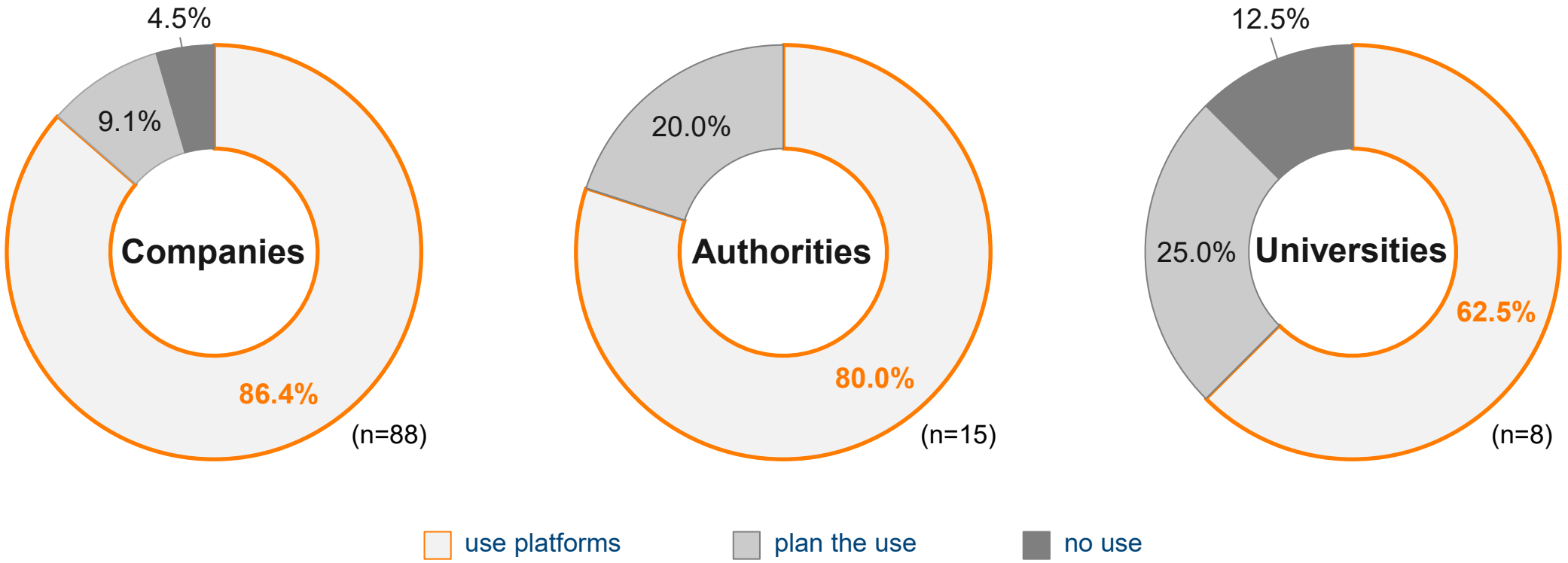


Widespread of Platforms in America and Europe



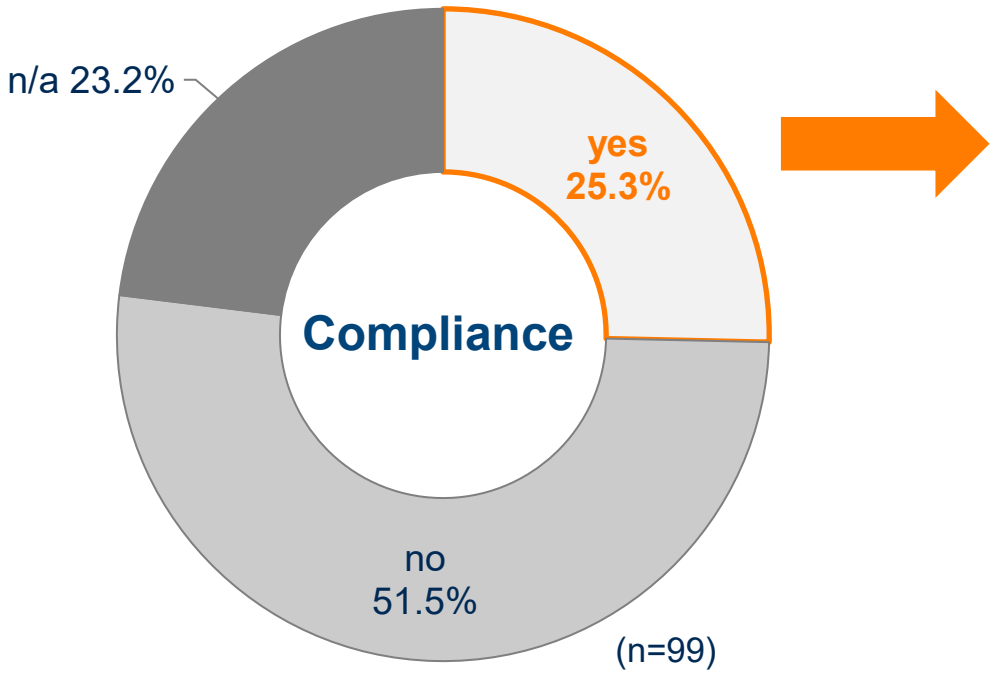
Platforms Are More Widespread in Companies Than in Authorities and Universities

What percentage of organisations use or plan to use threat intelligence sharing platforms?

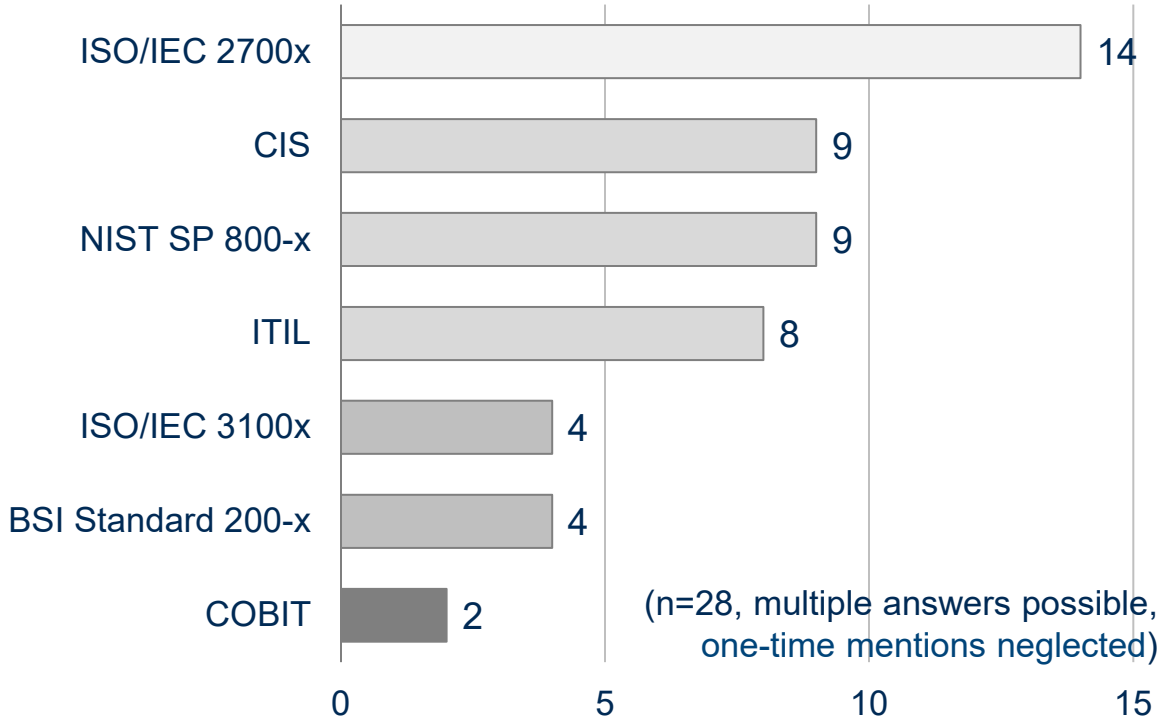


Compliance and Certification Requirements Are Not the Main Reasons for Using TISPs

Does your organisation use threat intelligence sharing platforms to comply with IT security and/or risk management standards?

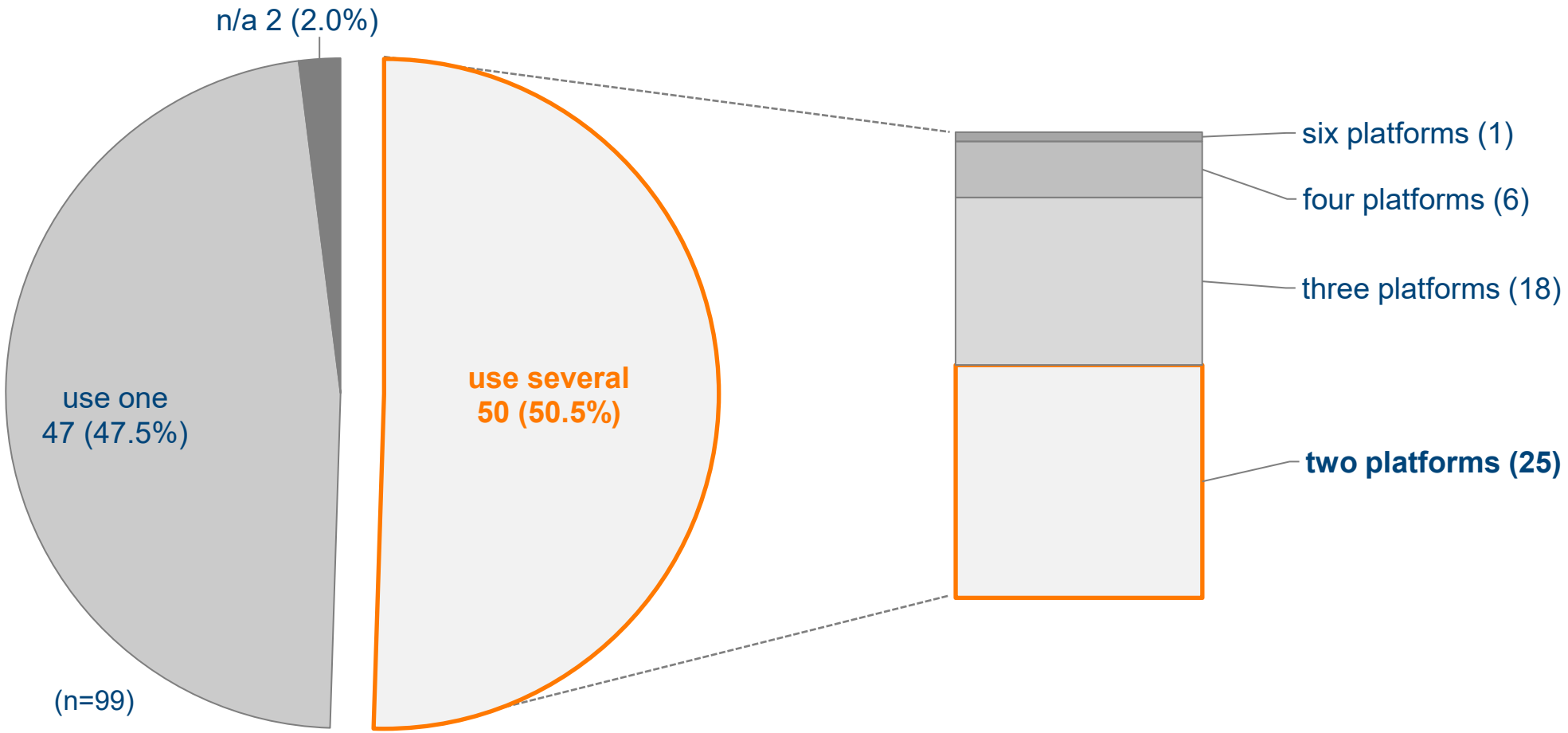


What compliance and certification requirements are met by organizations using TISPs because of them?

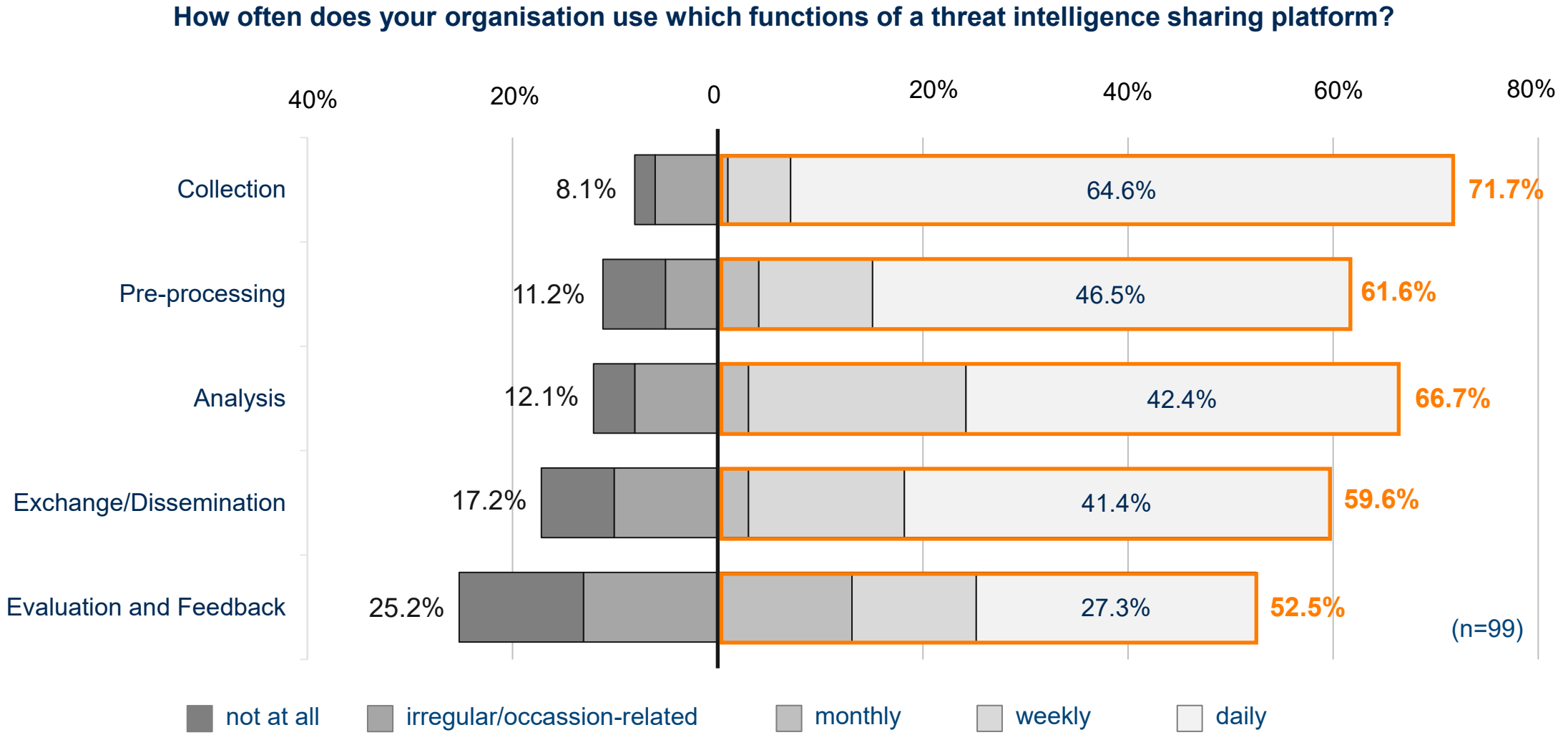


Simultaneous Use of Multiple Platforms Is Popular

What percentage of organisations use several threat intelligence sharing platforms simultaneously?



Platforms Are Regulary Used Not Only for the Collection, Pre-Processing, Analysis and Dissemination, but Also for Evaluation of TI



Conclusion and Outlook

- status quo on the widespread and statements on the use of threat intelligence sharing platforms worldwide
- explorative results only (no random sampling)
- strong focus on Europe & America

- repetition of the study (trend analyses)
- comparative country- and region-specific statements about the use of platforms

Insights on the Spread and Use of Threat Intelligence Sharing Platforms

Clemens Sauerwein* and Daniel Fischer°

* University of Innsbruck (Austria)
° Technische Universität Ilmenau (Germany)

06-03-2024

Security Interest Group Switzerland – 23rd SOC Forum

Hilton Zürich Airport, Switzerland

TLP:Green