2021 Annual Computer Security Applications Conference (ACSAC)
December 6-10, 2021 | Online

What’s in a Cyber Threat Intelligence sharing platform?

A mixed-methods user experience investigation of MISP

Borče Stojkovski
SnT, University of Luxembourg
borce.stojkovski@uni.lu

Gabriele Lenzini
SnT, University of Luxembourg
gabriele.lenzini@uni.lu

Vincent Koenig
COSA, University of Luxembourg
vincent.koenig@uni.lu

Salvador Rivas
COSA, University of Luxembourg
salvador.rivas@uni.lu

Authors are supported by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared

Outline

1 Introduction and Research Context

2 Use case (MISP) and User Study

3 Results and Analysis

4 Discussion and Future work

1 Introduction & Research Context

Growing number and sophistication of cyber attacks

INTERPOL

INTERPOL report shows alarming rate of cyberattacks during COVID-1

4 August 2020

The Pegasus project

Pegasus project: spyware leak suggests lawyers and activists at risk across globe

Leaked records show dissidents and those who help them prominent among those under threat from NSO spyware

infrastructure.

With organizations and businesses rapidly deploying remote systems and
working from home, criminals are also takin
data. generat

NEWS

Cyberattack on US Department of Energy a 'grave threat'

The attack is part of the huge SolarWinds hack that has hit other government agency systems and critical infrastructure. The US cybersecurity agency has warned it poses a serious risk.

developing and their attacks at an alarming pace, fear and uncertainty caused by th social and economic situation crea 19.”

Jürgen Stock, INTERPOL Secretary General

Axa’s Asian operations hit in ransomware attack

French insurer’s units in Thailand, Malaysia, Hong Kong and Philippines affected

FINANCIAL TIMES

Malicious software attacks ‘spiralling out of control’, report warns

UK has world’s secon
US

All types

Helen Wa

The Economist

Briefing

Crims and spooks unite and figh

Ransomware highlights the challenges and subtleties of cybersecurity

Governments want to defend themselves—and attack others

PRESS RELEASE

ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected

Threat landscape maps

the EU,
olding its
fuelling

SECURITY 03.05.2021 06:56 PM

Hit an ‘Astronomical’

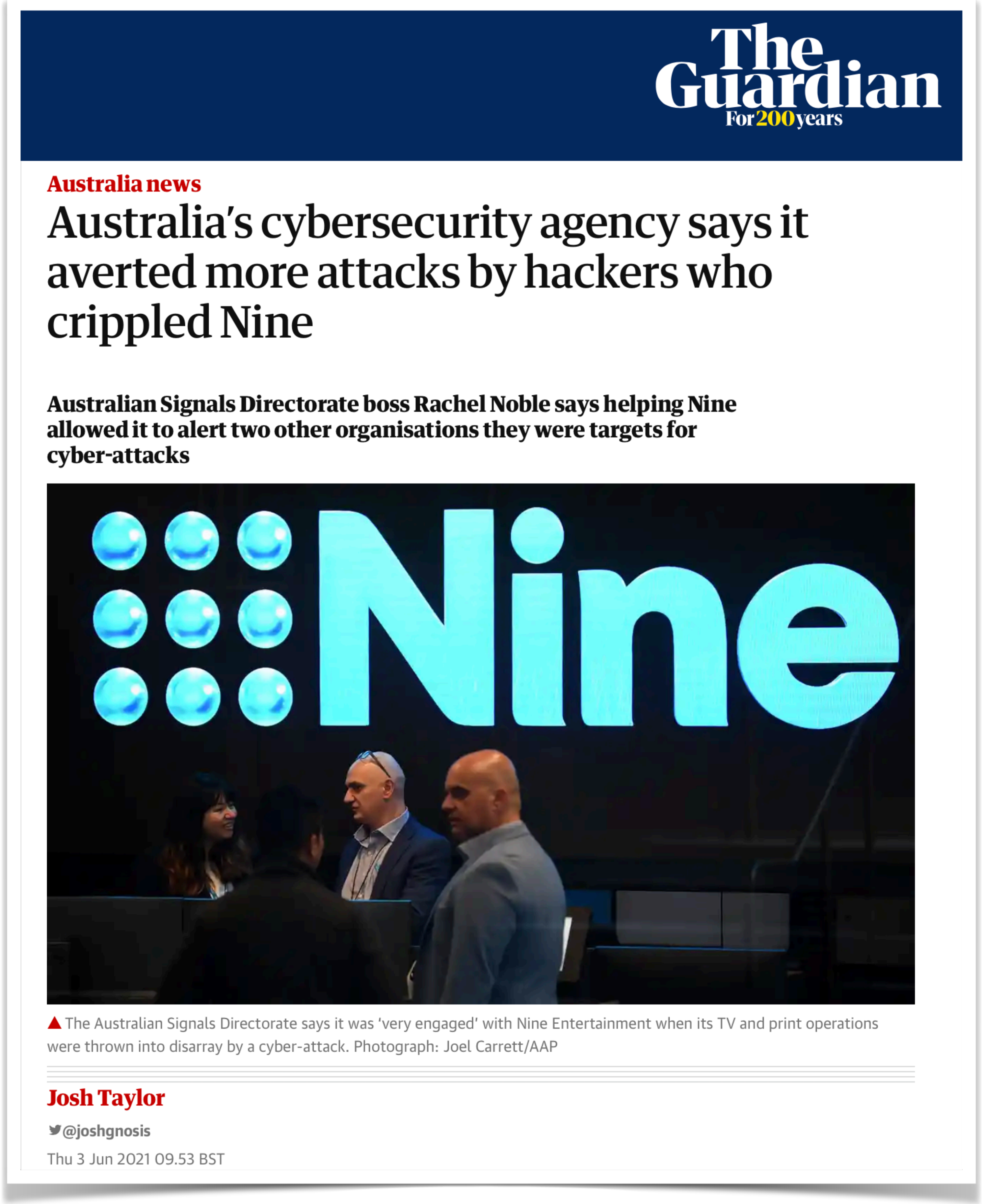
tens of thousands of Microsoft

allowed
upt Colonial
peline, CEO tells senators

INTERNET ORGANISED CRIME THREAT ASSESSMENT 2021

In this year’s report, the impact of the COVID-19 pandemic remains visible. Cybercriminals have continued exploiting opportunities created by lockdowns and continued teleworking. Ransomware affiliate programs have increased in prominence and are tied to a multitude of high-profile attacks against healthcare institutions and services providers.

Growing number and sophistication of cyber attacks



The Guardian
For 200 years

Australia news

Australia's cybersecurity agency says it averted more attacks by hackers who crippled Nine

Australian Signals Directorate boss Rachel Noble says helping Nine allowed it to alert two other organisations they were targets for cyber-attacks

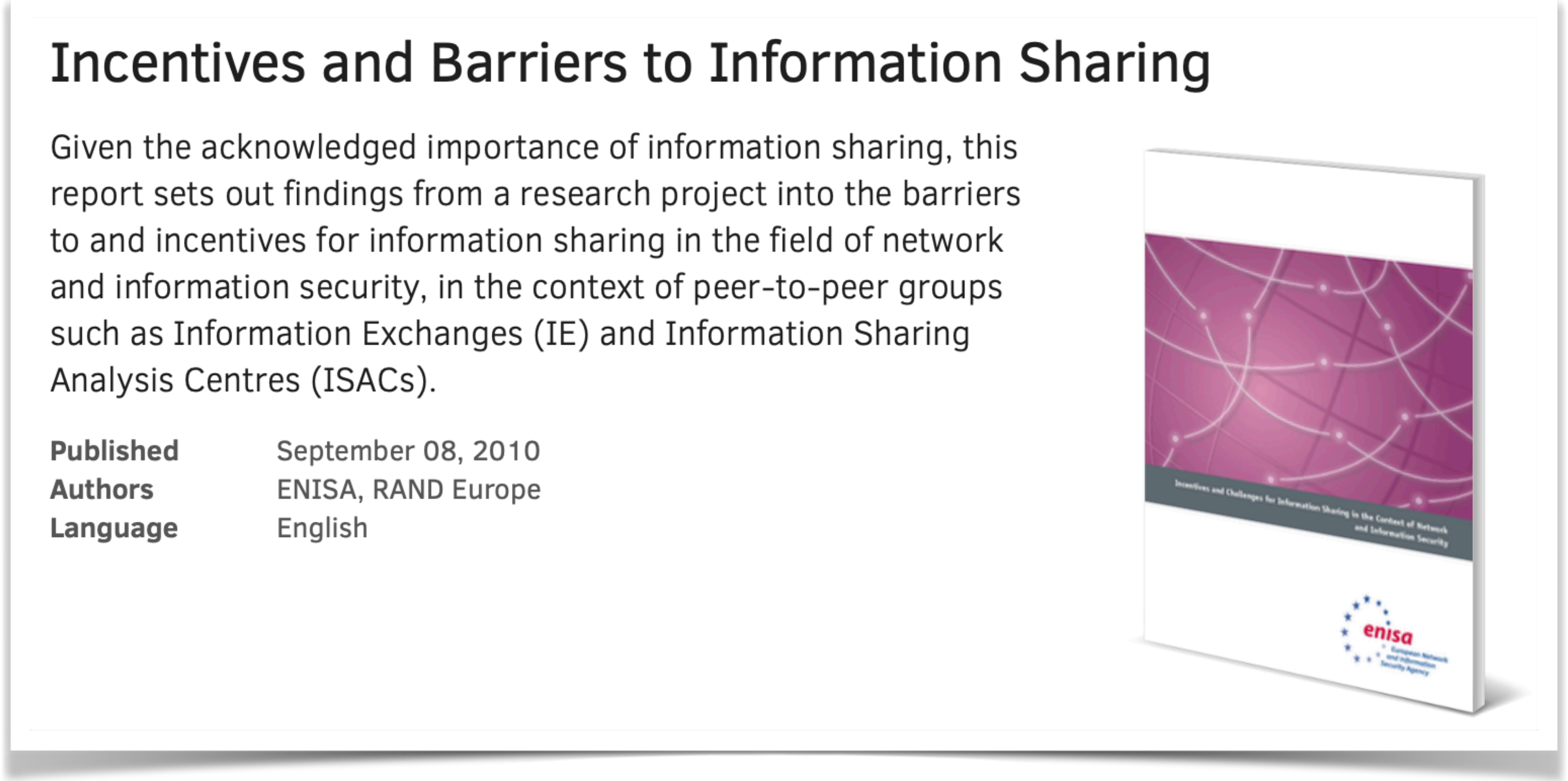
▲ The Australian Signals Directorate says it was 'very engaged' with Nine Entertainment when its TV and print operations were thrown into disarray by a cyber-attack. Photograph: Joel Carrett/AAP

Josh Taylor
@joshgnosis
Thu 3 Jun 2021 09.53 BST

EUROPOL

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

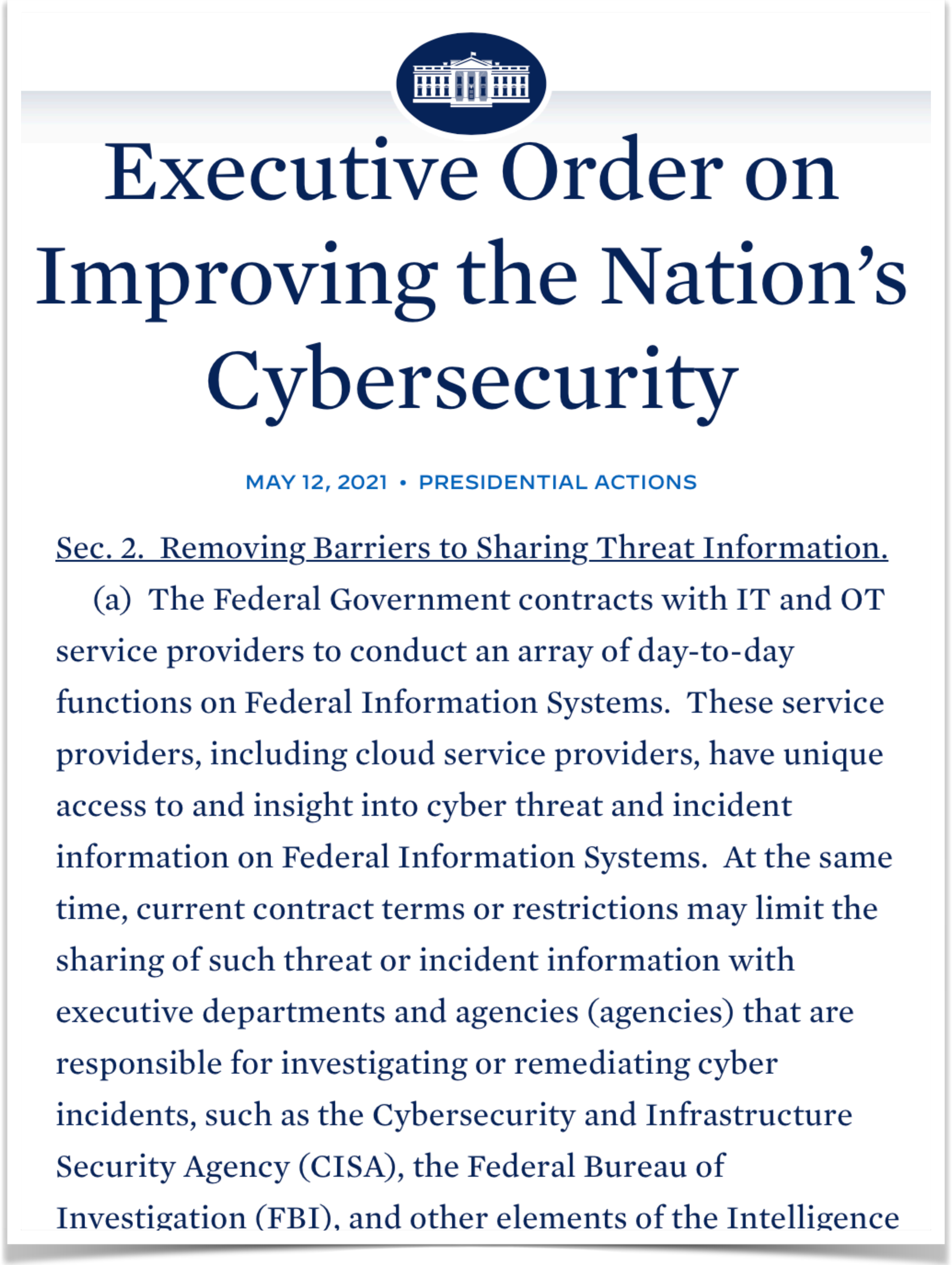
27 Jan 2021



Incentives and Barriers to Information Sharing

Given the acknowledged importance of information sharing, this report sets out findings from a research project into the barriers to and incentives for information sharing in the field of network and information security, in the context of peer-to-peer groups such as Information Exchanges (IE) and Information Sharing Analysis Centres (ISACs).

Published	September 08, 2010
Authors	ENISA, RAND Europe
Language	English



Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

Sec. 2. Removing Barriers to Sharing Threat Information.

(a) The Federal Government contracts with IT and OT service providers to conduct an array of day-to-day functions on Federal Information Systems. These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence

Cyber Threat Intelligence Sharing

- Countermeasure to the **growing number** and **sophistication** of attacks in different cyber security scenarios
  - financially-driven cyber criminal activities, cyberwar, hacktivism, terrorism, etc.

Cyber Threat Intelligence Sharing

- Countermeasure to the **growing number** and **sophistication** of attacks in different cyber security scenarios
  - financially-driven cyber criminal activities, cyberwar, hacktivism, terrorism, etc.
- However, **complicated** by a number of technical, organizational, legal, economical, and social barriers and challenges
  - Emergence of Standards for formatting CTI information and Sharing Platforms

CTI Standards and Sharing Platforms

- STIX
- TAXII
- OTX
- IODEF
- CyBOX
- OpenTPX
- RID
- VERIS
- *etc.*

- Anomali STAXX
- CRITs
- OpenCTI
- MISP
- EclecticIQ
- CIF
- Threat Connect
- IBM X-Force
- *etc.*

Human, cultural & organizational aspects

- Nature of the job, organizational setting, tools and workflows of IT security professionals
- Collaborative work practices in the CTI (sharing) context
- Motivation
- Skills development
- Usability and User Experience (UX)

Motivation for our work

- **Importance of UX:** empirical evidence on the usability, or perceived UX of CTI sharing platforms is scarce to non-existent
- **Knowledge gap** regarding users' perceptions of key tasks
  - enabling and constraining factors of security information sharing
  - how much effective CTI sharing is impacted by usability problems or UX

Contribution

- **Empirical**
  - First UX benchmark for a leading CTI sharing platform
  - Key findings and UX recommendations of relevance to CTI sharing platforms in general
  - Possible negative outcomes in terms of security and adoption related to UX
- **Methodological**
  - Demonstration of the utility and necessity of UX research methods in cybersecurity

2 Use case (MISP) & User study

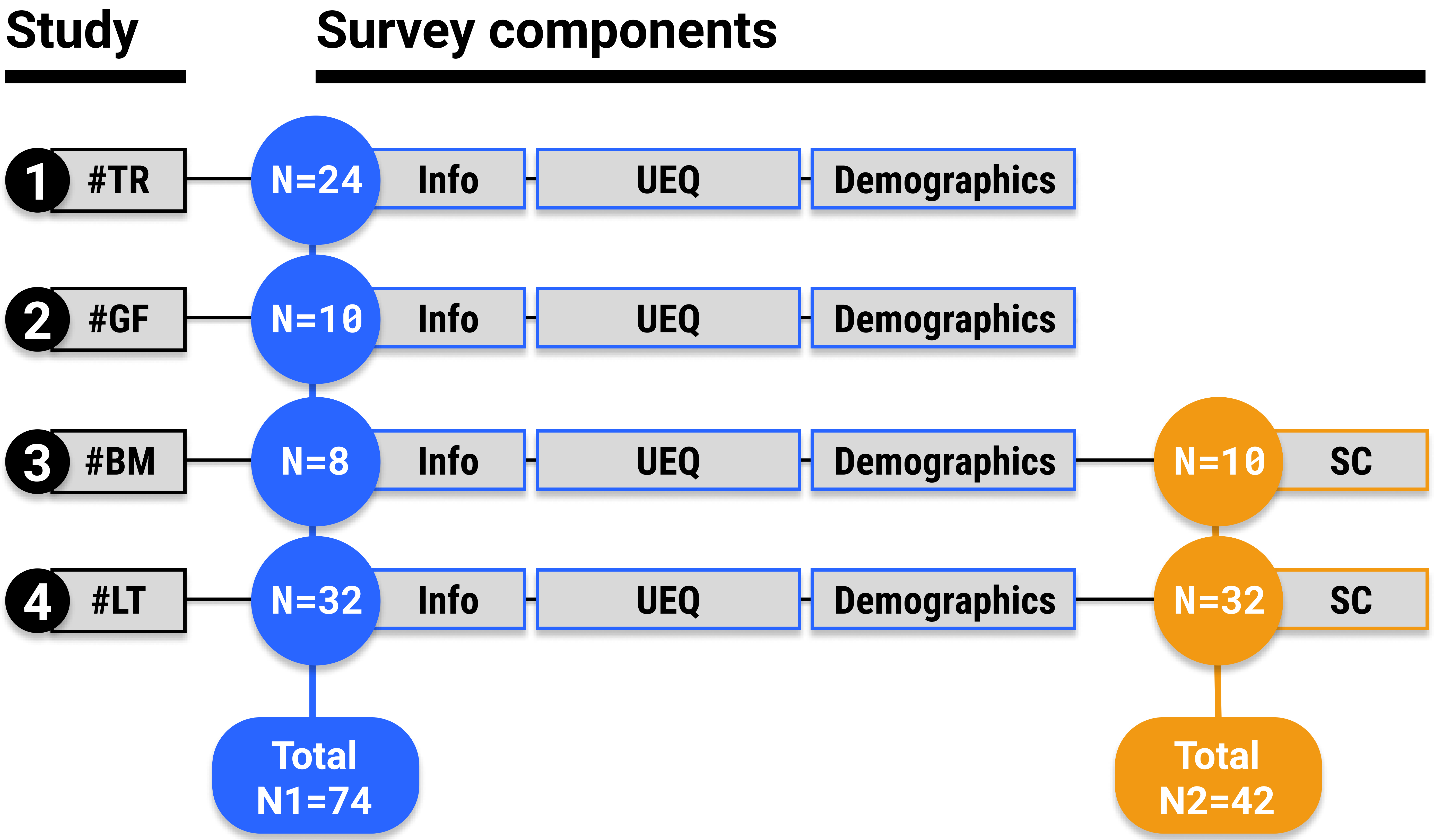
MISP

- A **leading** open-source CTI sharing platform
  - Inception within military circles 15 years ago
  - Used by over 6,000 organizations worldwide
  - UI and API users
  - Characterized as holistic and applicable in diverse scenarios (De Melo e Silva et al., 2020)
- More info: https://www.misp-project.org

Research Questions

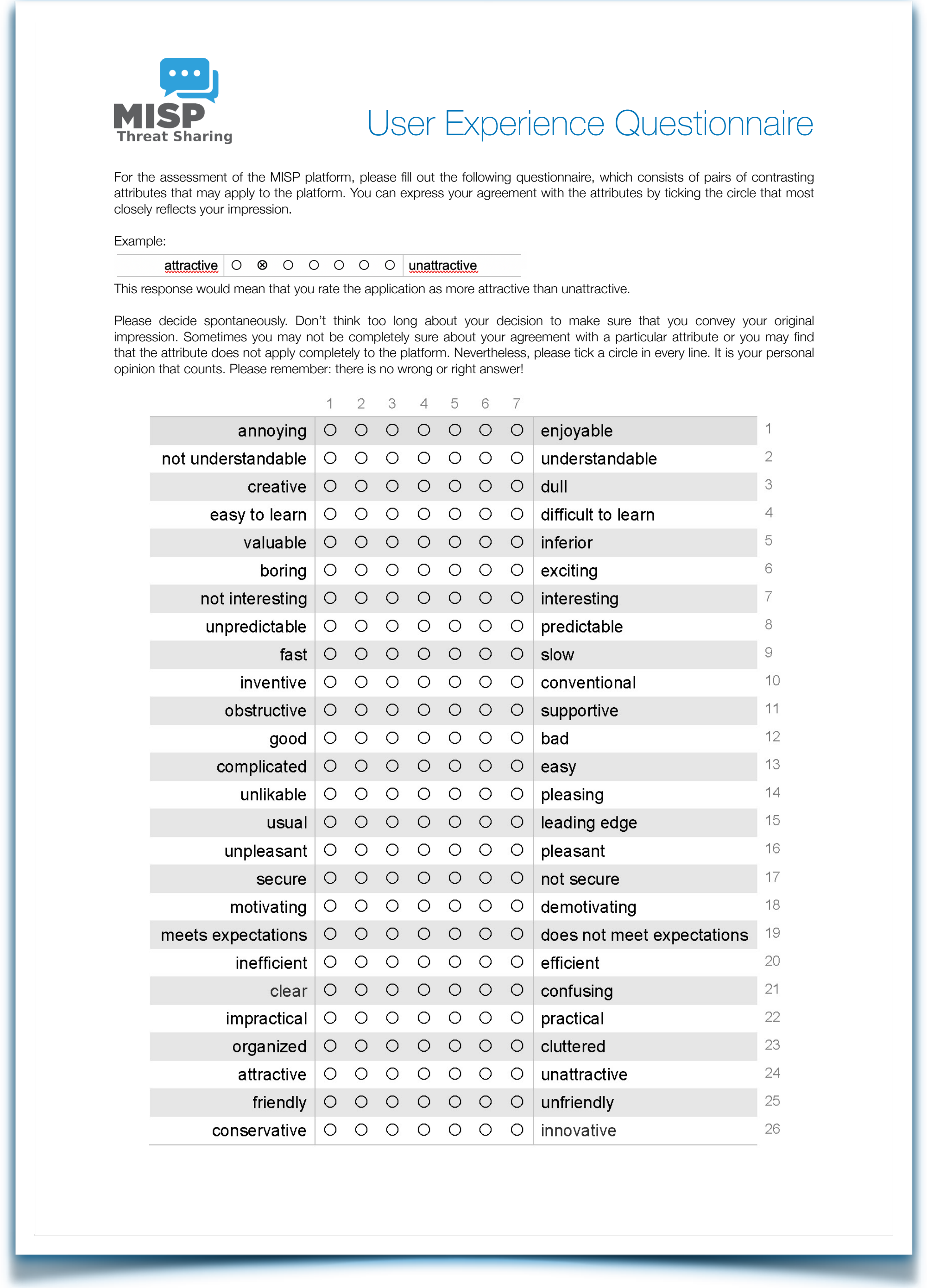
- How do different security information workers evaluate the UX of MISP?
- What do users value about MISP and what do they think could be improved?
- Which user needs are addressed and accounted for by MISP, and which are neglected?

Methodology



Study		Survey components					
1	#TR	N=24	Info	UEQ	Demographics		
2	#GF	N=10	Info	UEQ	Demographics		
3	#BM	N=8	Info	UEQ	Demographics	N=10	SC
4	#LT	N=32	Info	UEQ	Demographics	N=32	SC
		Total N1=74				Total N2=42	

Methodology



MISP Threat Sharing

User Experience Questionnaire

For the assessment of the MISP platform, please fill out the following questionnaire, which consists of pairs of contrasting attributes that may apply to the platform. You can express your agreement with the attributes by ticking the circle that most closely reflects your impression.

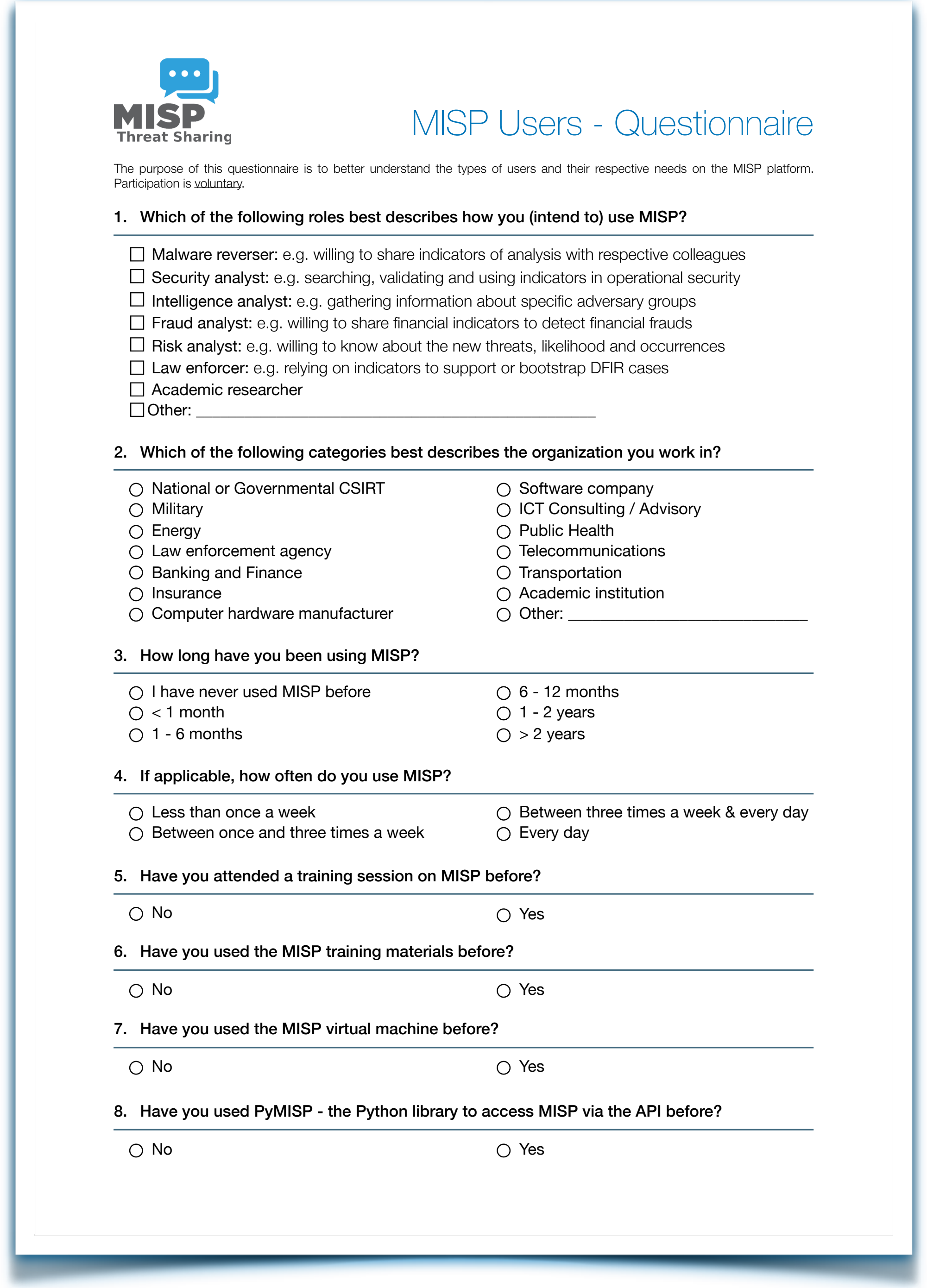
Example:

attractive ○ ⊗ ○ ○ ○ ○ ○ unattractive

This response would mean that you rate the application as more attractive than unattractive.

Please decide spontaneously. Don't think too long about your decision to make sure that you convey your original impression. Sometimes you may not be completely sure about your agreement with a particular attribute or you may find that the attribute does not apply completely to the platform. Nevertheless, please tick a circle in every line. It is your personal opinion that counts. Please remember: there is no wrong or right answer!

	1	2	3	4	5	6	7		
annoying	○	○	○	○	○	○	○	enjoyable	1
not understandable	○	○	○	○	○	○	○	understandable	2
creative	○	○	○	○	○	○	○	dull	3
easy to learn	○	○	○	○	○	○	○	difficult to learn	4
valuable	○	○	○	○	○	○	○	inferior	5
boring	○	○	○	○	○	○	○	exciting	6
not interesting	○	○	○	○	○	○	○	interesting	7
unpredictable	○	○	○	○	○	○	○	predictable	8
fast	○	○	○	○	○	○	○	slow	9
inventive	○	○	○	○	○	○	○	conventional	10
obstructive	○	○	○	○	○	○	○	supportive	11
good	○	○	○	○	○	○	○	bad	12
complicated	○	○	○	○	○	○	○	easy	13
unlikable	○	○	○	○	○	○	○	pleasing	14
usual	○	○	○	○	○	○	○	leading edge	15
unpleasant	○	○	○	○	○	○	○	pleasant	16
secure	○	○	○	○	○	○	○	not secure	17
motivating	○	○	○	○	○	○	○	demotivating	18
meets expectations	○	○	○	○	○	○	○	does not meet expectations	19
inefficient	○	○	○	○	○	○	○	efficient	20
clear	○	○	○	○	○	○	○	confusing	21
impractical	○	○	○	○	○	○	○	practical	22
organized	○	○	○	○	○	○	○	cluttered	23
attractive	○	○	○	○	○	○	○	unattractive	24
friendly	○	○	○	○	○	○	○	unfriendly	25
conservative	○	○	○	○	○	○	○	innovative	26



MISP Threat Sharing

MISP Users - Questionnaire

The purpose of this questionnaire is to better understand the types of users and their respective needs on the MISP platform. Participation is voluntary.

1. Which of the following roles best describes how you (intend to) use MISP?

- □ **Malware reverser:** e.g. willing to share indicators of analysis with respective colleagues
- □ **Security analyst:** e.g. searching, validating and using indicators in operational security
- □ **Intelligence analyst:** e.g. gathering information about specific adversary groups
- □ **Fraud analyst:** e.g. willing to share financial indicators to detect financial frauds
- □ **Risk analyst:** e.g. willing to know about the new threats, likelihood and occurrences
- □ **Law enforcer:** e.g. relying on indicators to support or bootstrap DFIR cases
- □ Academic researcher
- □ Other: ____________________________________

2. Which of the following categories best describes the organization you work in?

- ○ National or Governmental CSIRT
- ○ Military
- ○ Energy
- ○ Law enforcement agency
- ○ Banking and Finance
- ○ Insurance
- ○ Computer hardware manufacturer
- ○ Software company
- ○ ICT Consulting / Advisory
- ○ Public Health
- ○ Telecommunications
- ○ Transportation
- ○ Academic institution
- ○ Other: ______________________

3. How long have you been using MISP?

- ○ I have never used MISP before
- ○ < 1 month
- ○ 1 - 6 months
- ○ 6 - 12 months
- ○ 1 - 2 years
- ○ > 2 years

4. If applicable, how often do you use MISP?

- ○ Less than once a week
- ○ Between once and three times a week
- ○ Between three times a week & every day
- ○ Every day

5. Have you attended a training session on MISP before?

○ No ○ Yes

6. Have you used the MISP training materials before?

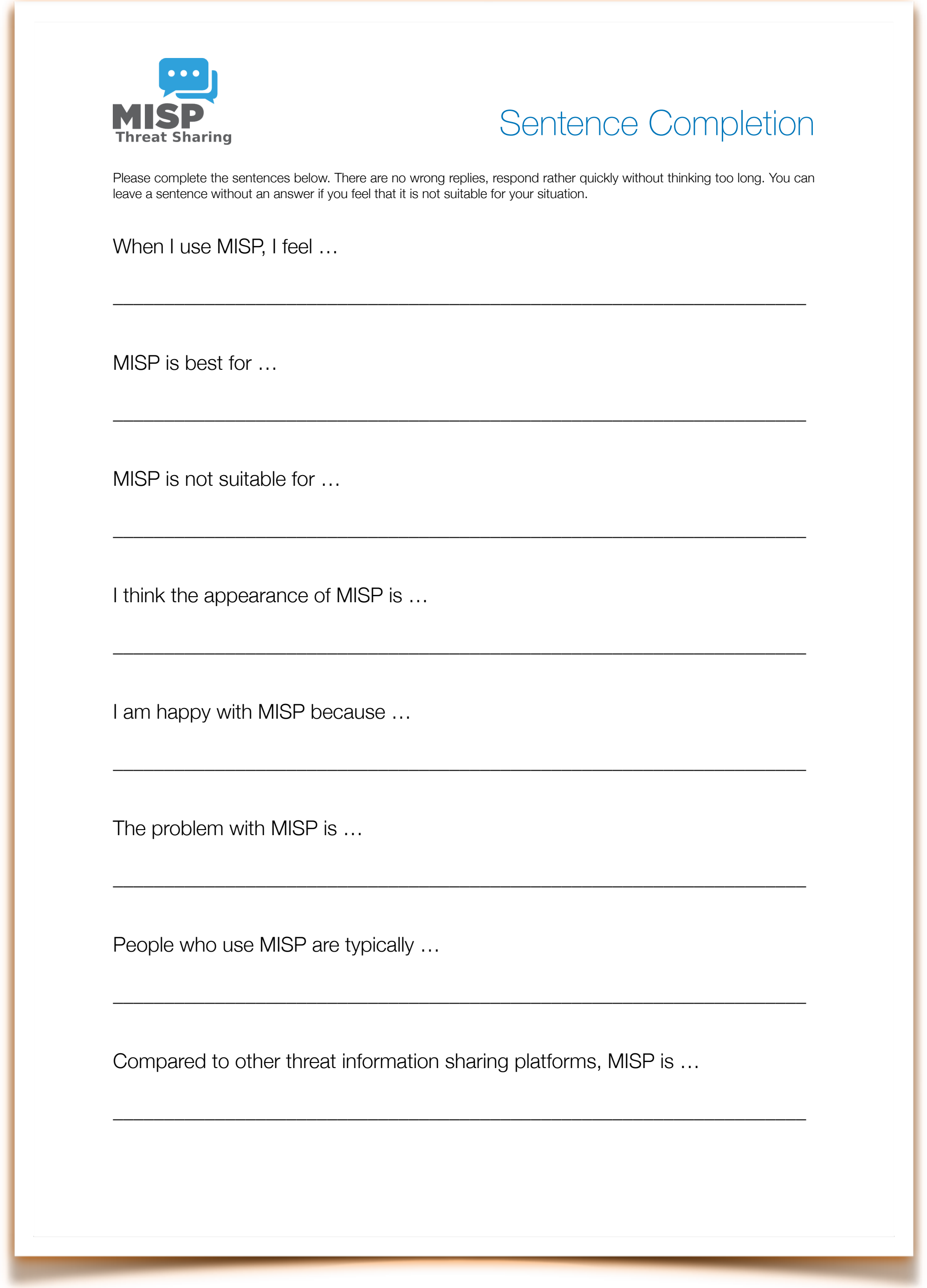
○ No ○ Yes

7. Have you used the MISP virtual machine before?

○ No ○ Yes

8. Have you used PyMISP - the Python library to access MISP via the API before?

○ No ○ Yes



MISP Threat Sharing

Sentence Completion

Please complete the sentences below. There are no wrong replies, respond rather quickly without thinking too long. You can leave a sentence without an answer if you feel that it is not suitable for your situation.

When I use MISP, I feel …

____

MISP is best for …

____

MISP is not suitable for …

____

I think the appearance of MISP is …

____

I am happy with MISP because …

____

The problem with MISP is …

____

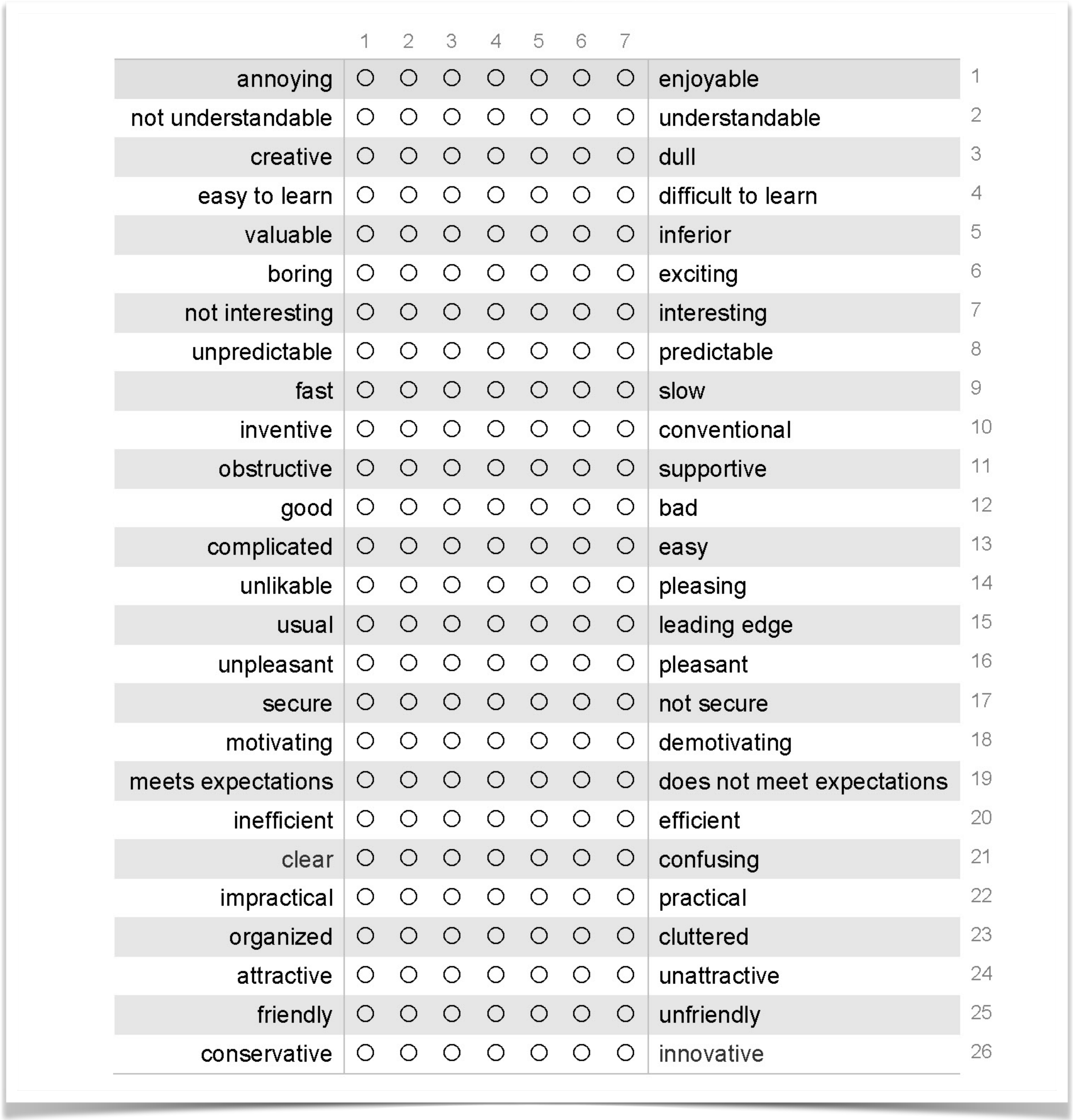
People who use MISP are typically …

____

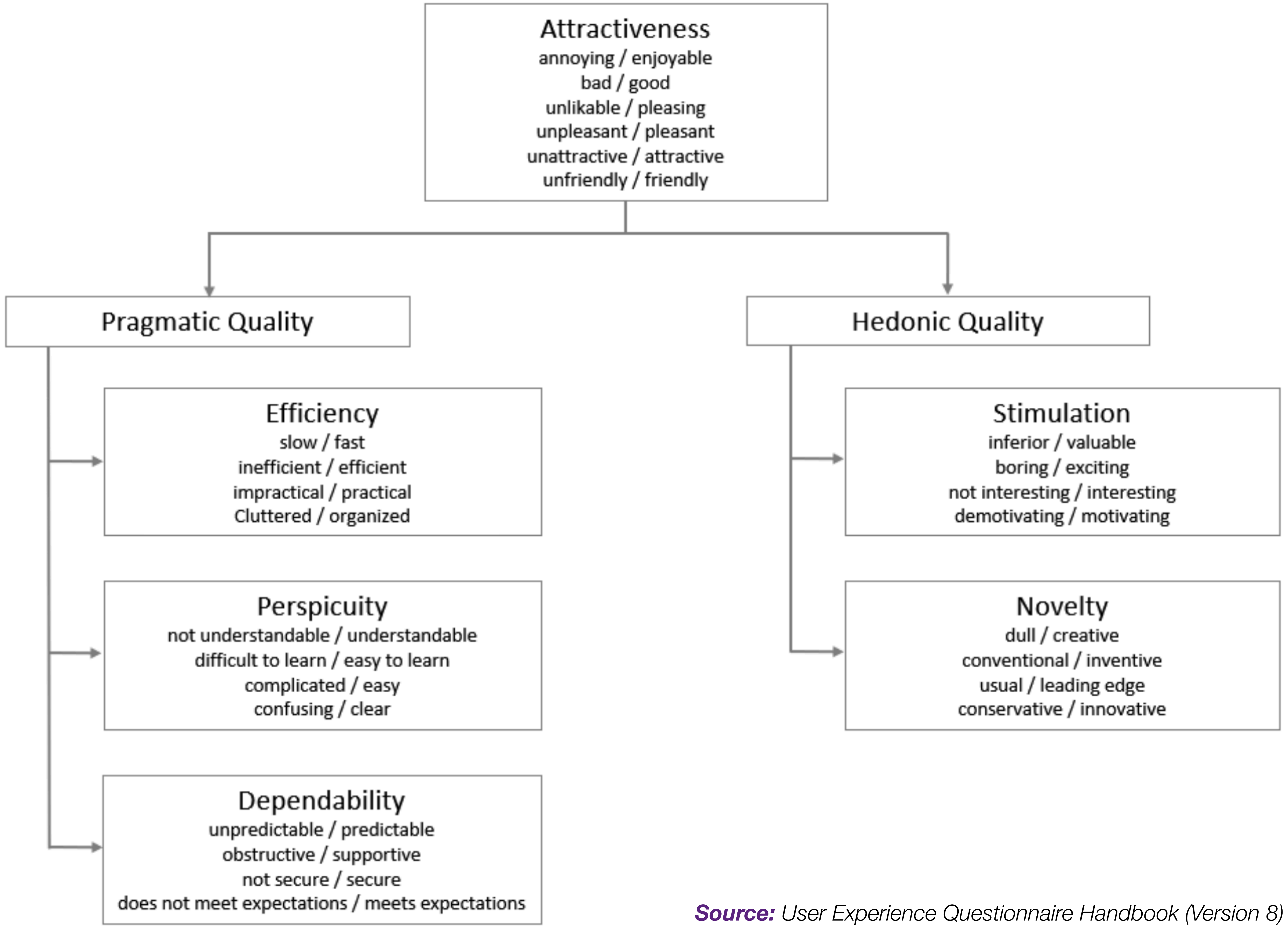
Compared to other threat information sharing platforms, MISP is …

____

Methodology - User Experience Questionnaire



	1	2	3	4	5	6	7		
annoying	○	○	○	○	○	○	○	enjoyable	1
not understandable	○	○	○	○	○	○	○	understandable	2
creative	○	○	○	○	○	○	○	dull	3
easy to learn	○	○	○	○	○	○	○	difficult to learn	4
valuable	○	○	○	○	○	○	○	inferior	5
boring	○	○	○	○	○	○	○	exciting	6
not interesting	○	○	○	○	○	○	○	interesting	7
unpredictable	○	○	○	○	○	○	○	predictable	8
fast	○	○	○	○	○	○	○	slow	9
inventive	○	○	○	○	○	○	○	conventional	10
obstructive	○	○	○	○	○	○	○	supportive	11
good	○	○	○	○	○	○	○	bad	12
complicated	○	○	○	○	○	○	○	easy	13
unlikable	○	○	○	○	○	○	○	pleasing	14
usual	○	○	○	○	○	○	○	leading edge	15
unpleasant	○	○	○	○	○	○	○	pleasant	16
secure	○	○	○	○	○	○	○	not secure	17
motivating	○	○	○	○	○	○	○	demotivating	18
meets expectations	○	○	○	○	○	○	○	does not meet expectations	19
inefficient	○	○	○	○	○	○	○	efficient	20
clear	○	○	○	○	○	○	○	confusing	21
impractical	○	○	○	○	○	○	○	practical	22
organized	○	○	○	○	○	○	○	cluttered	23
attractive	○	○	○	○	○	○	○	unattractive	24
friendly	○	○	○	○	○	○	○	unfriendly	25
conservative	○	○	○	○	○	○	○	innovative	26



Attractiveness
annoying / enjoyable
bad / good
unlikable / pleasing
unpleasant / pleasant
unattractive / attractive
unfriendly / friendly

Pragmatic Quality

Hedonic Quality

Efficiency
slow / fast
inefficient / efficient
impractical / practical
Cluttered / organized

Perspicuity
not understandable / understandable
difficult to learn / easy to learn
complicated / easy
confusing / clear

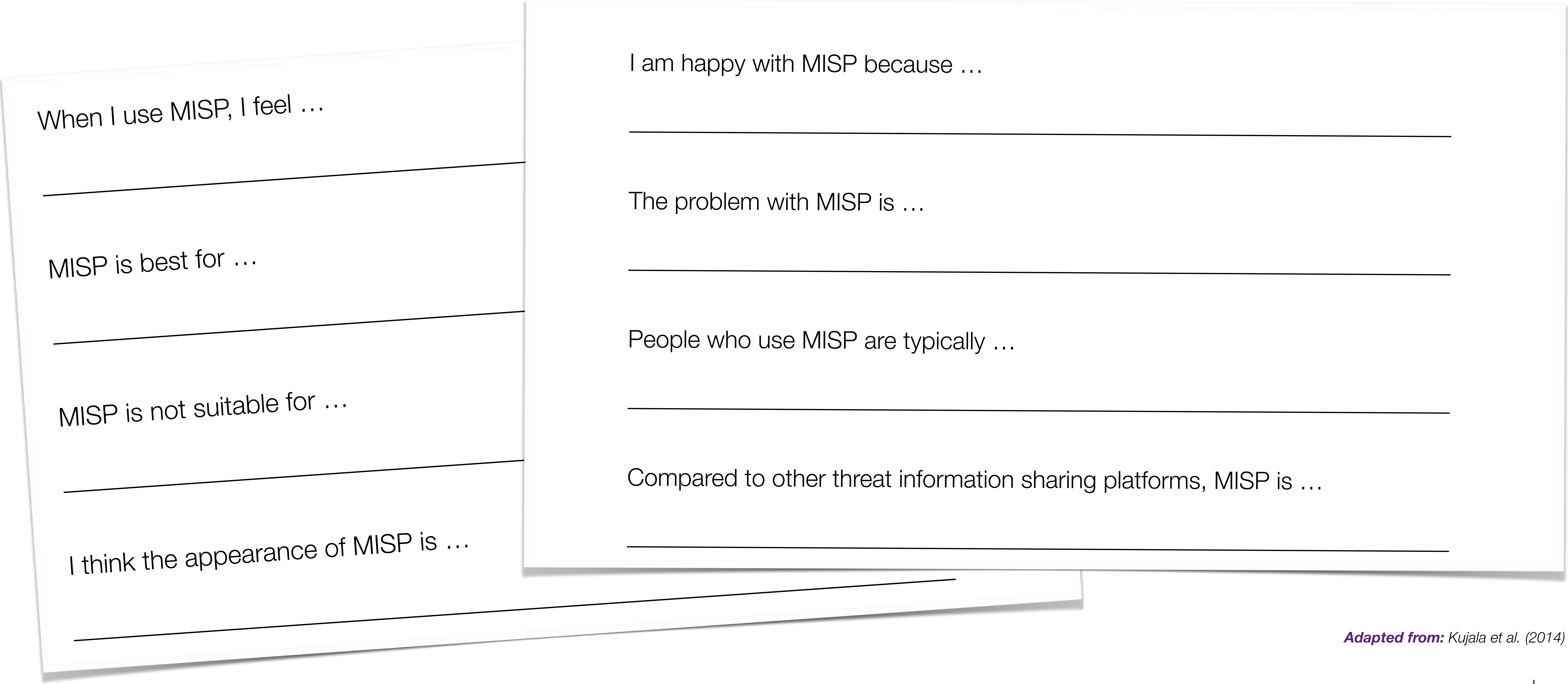
Dependability
unpredictable / predictable
obstructive / supportive
not secure / secure
does not meet expectations / meets expectations

Stimulation
inferior / valuable
boring / exciting
not interesting / interesting
demotivating / motivating

Novelty
dull / creative
conventional / inventive
usual / leading edge
conservative / innovative

Source: *User Experience Questionnaire Handbook (Version 8)*

Methodology - Sentence Completion



When I use MISP, I feel …

MISP is best for …

MISP is not suitable for …

I think the appearance of MISP is …

I am happy with MISP because …

The problem with MISP is …

People who use MISP are typically …

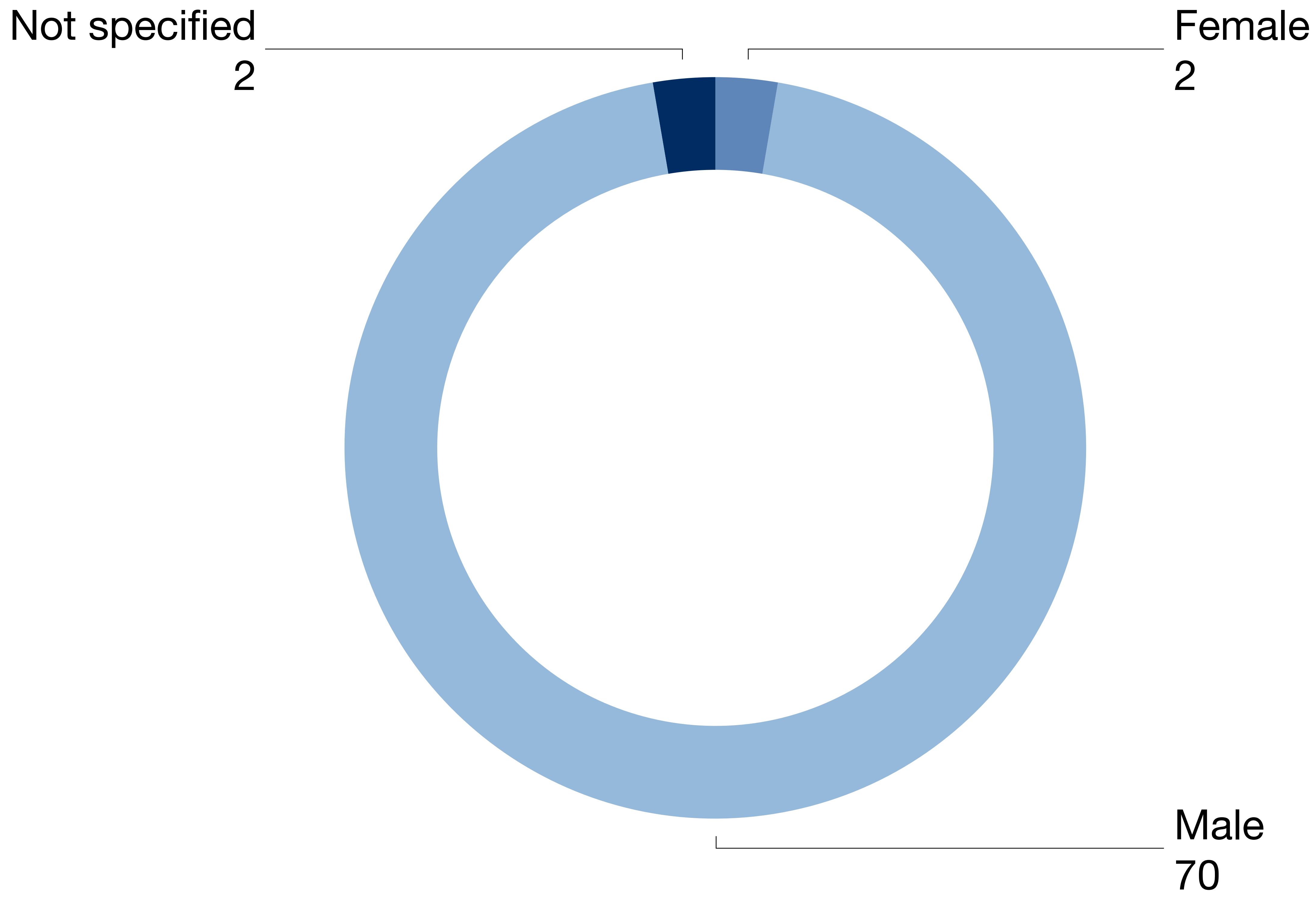
Compared to other threat information sharing platforms, MISP is …

Adapted from: *Kujala et al. (2014)*

3 Results and Analysis

Participants

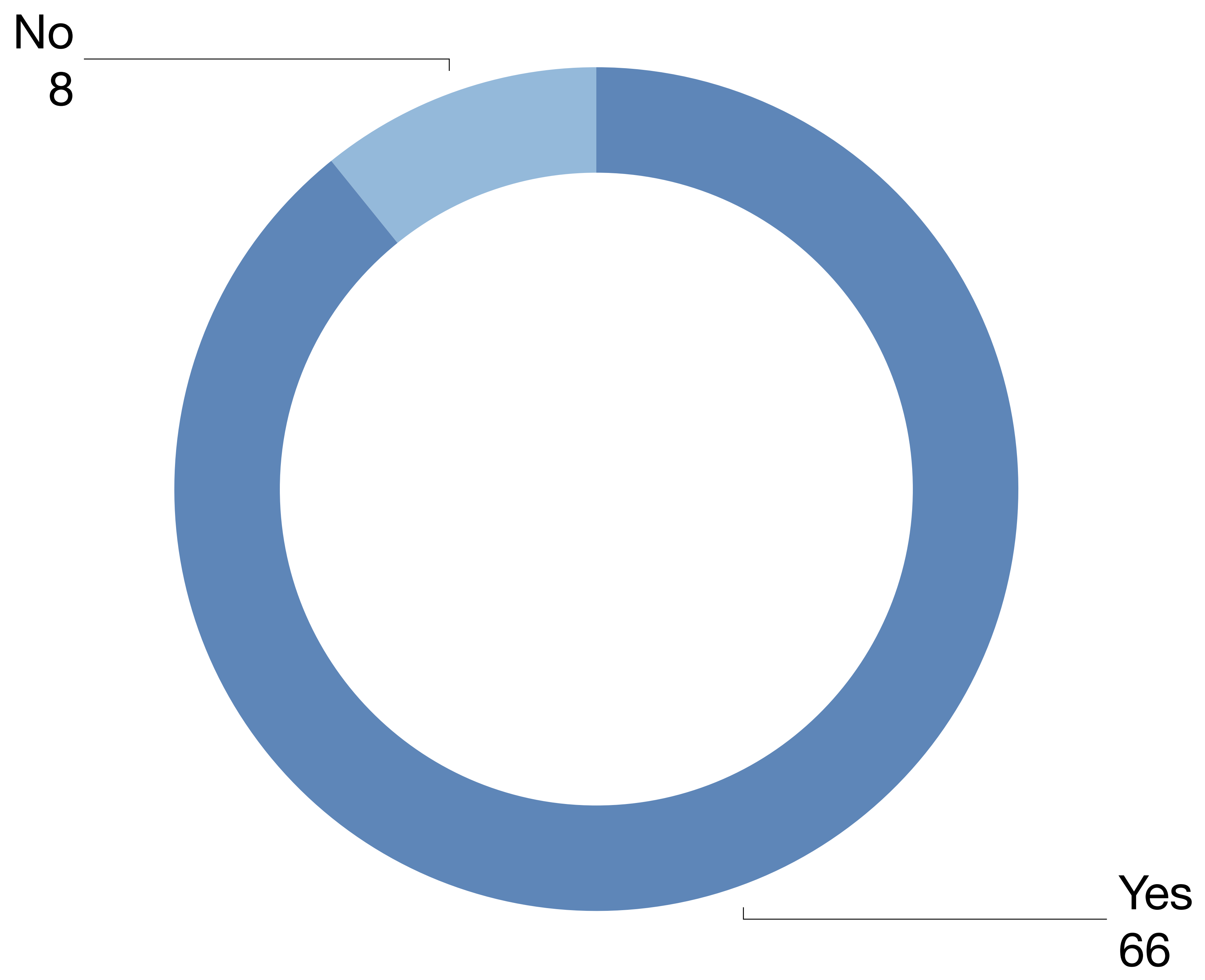
Gender



N=74

Participants

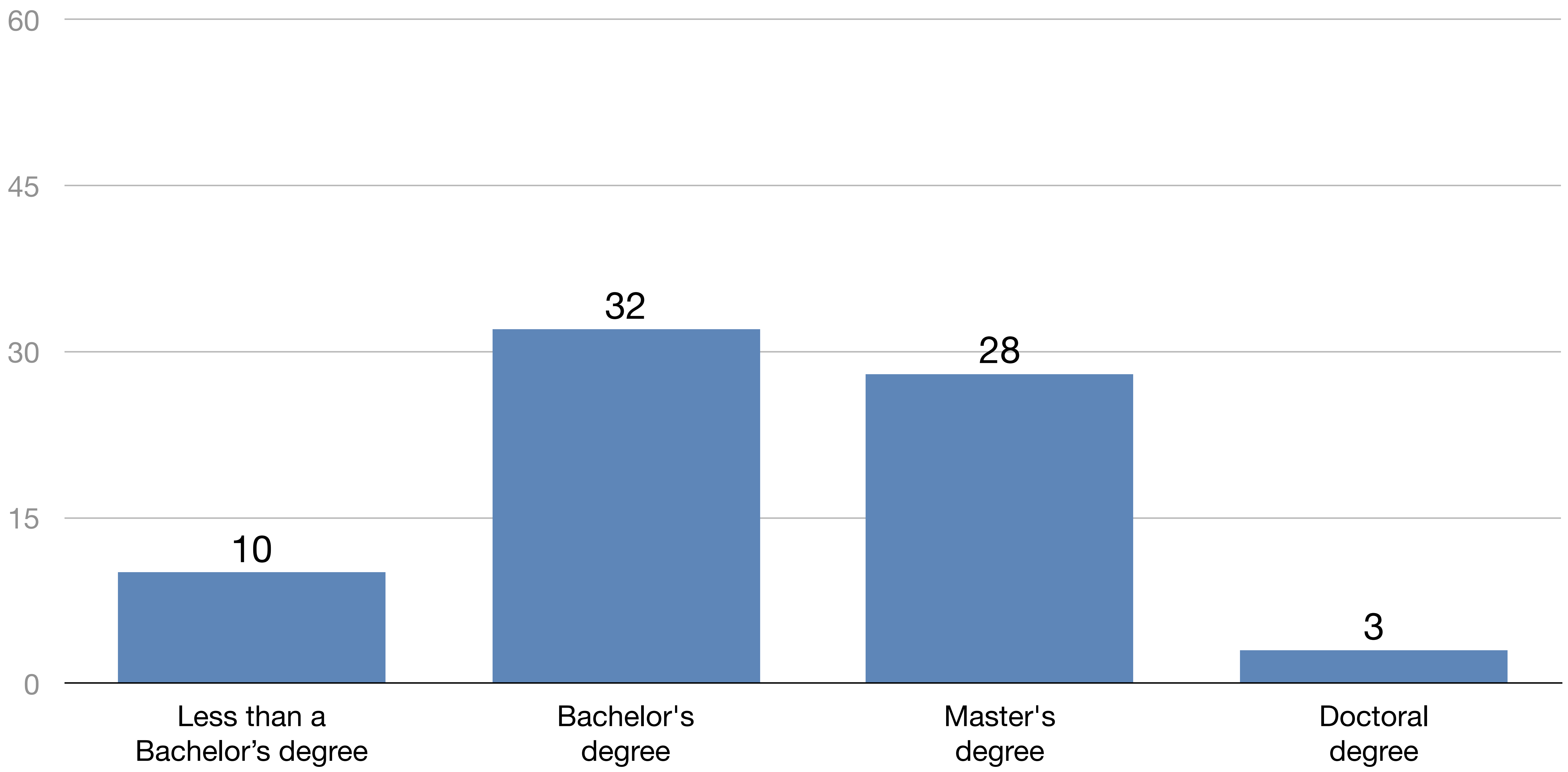
Engineering / Tech Background



N=74

Participants

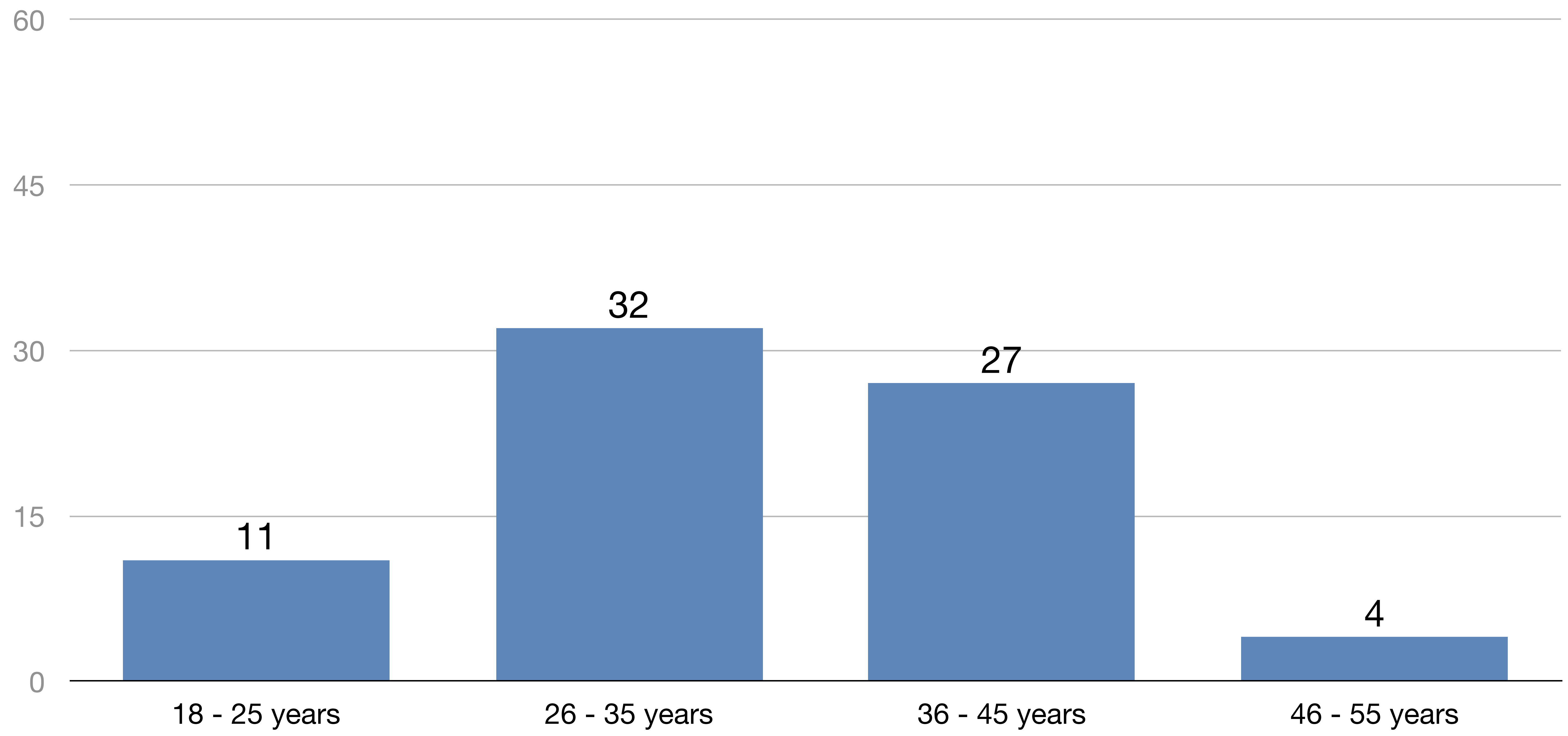
Education



N=73

Participants

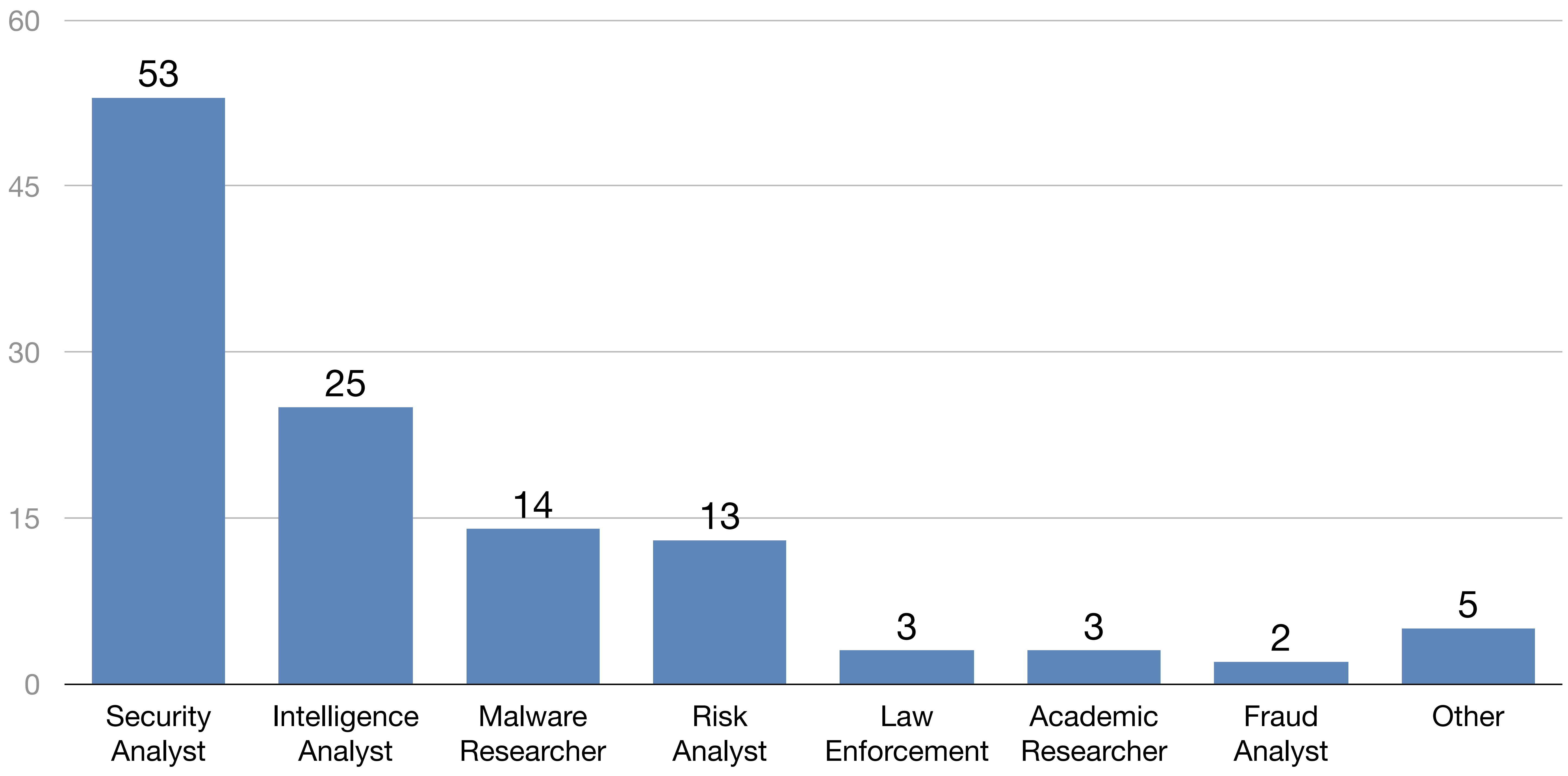
Age Group



N=74

Participants

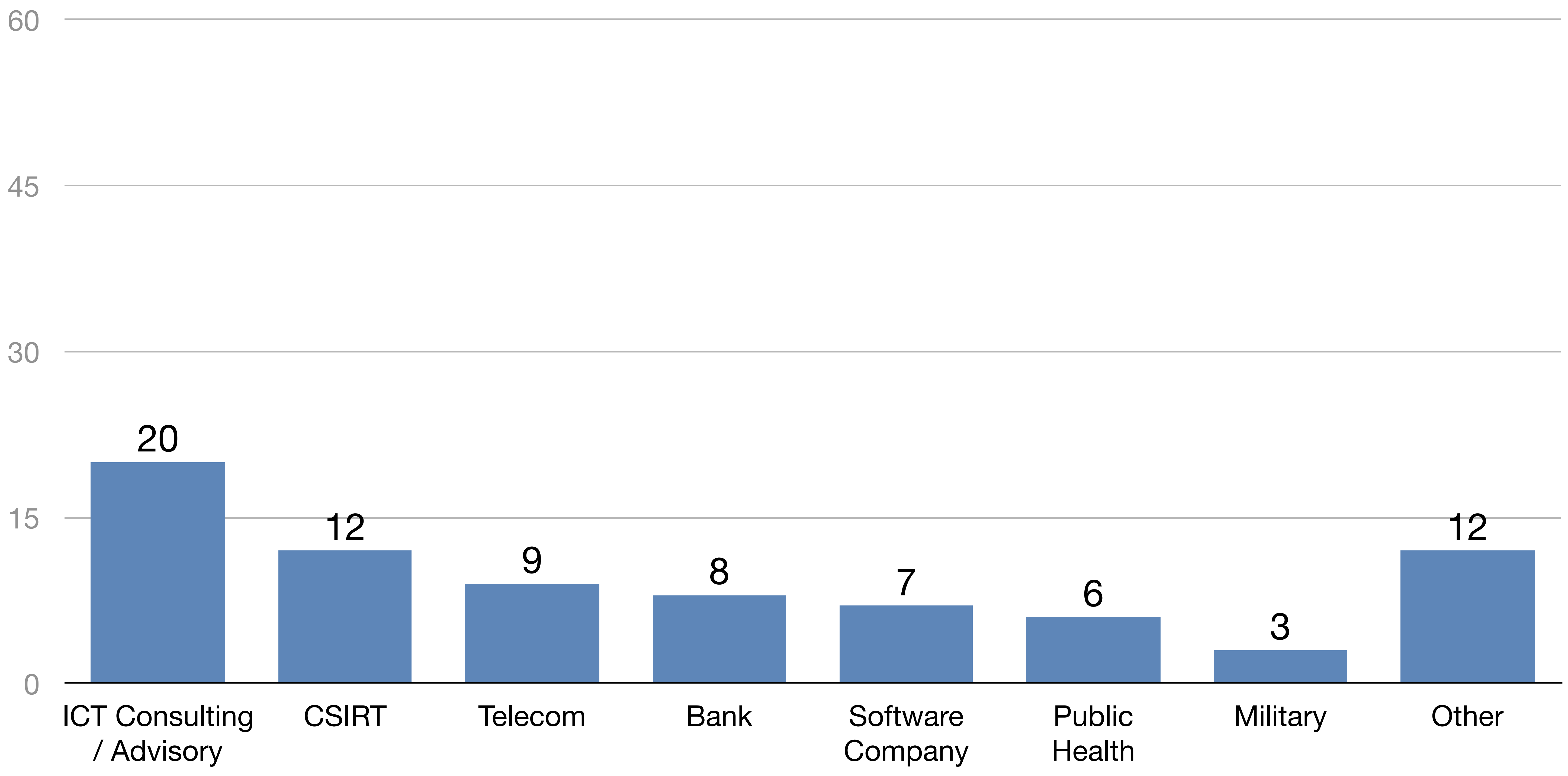
Role (multiple possible)



N=74

Participants

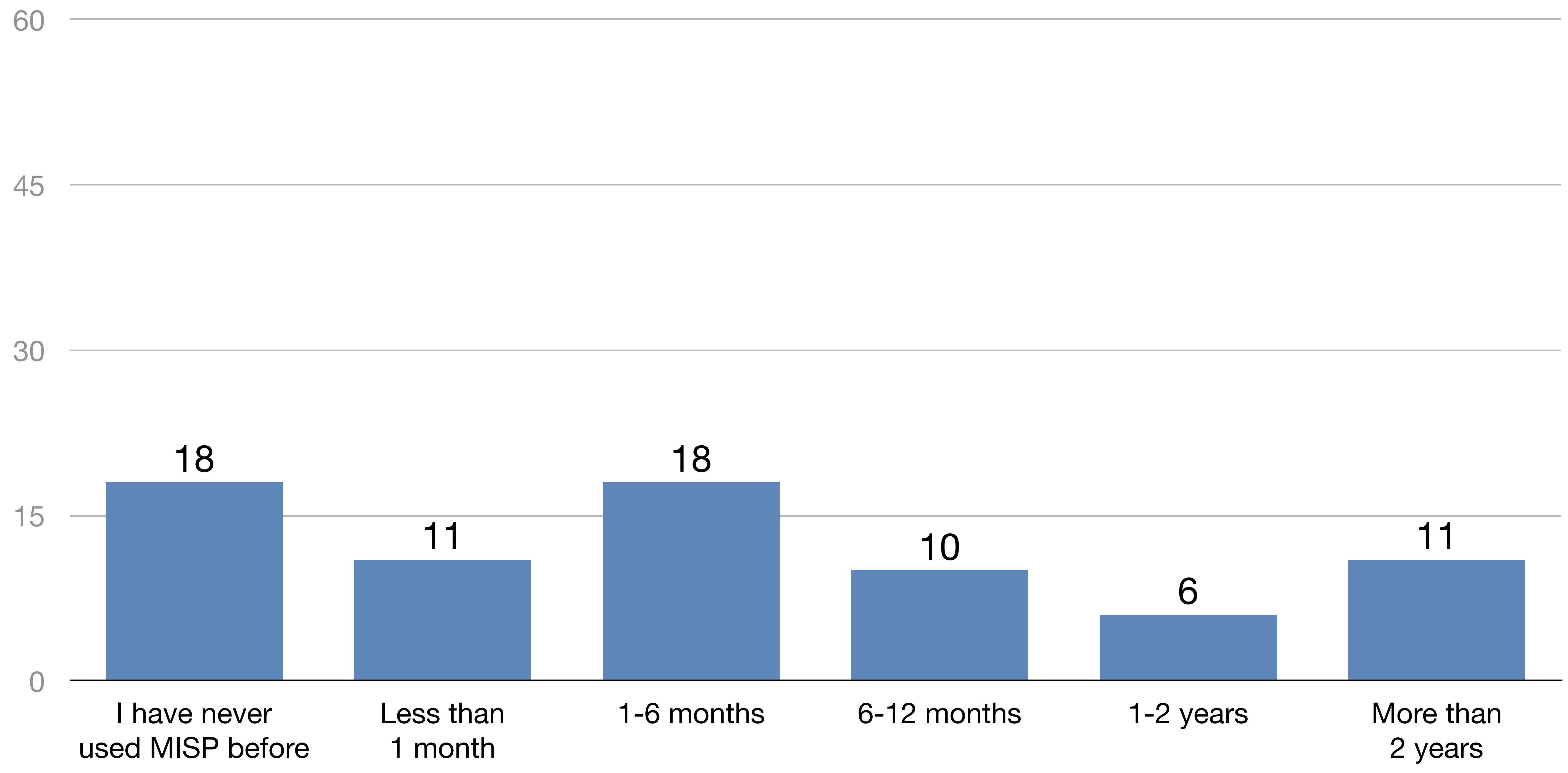
Industry (multiple possible)



N=74

Participants

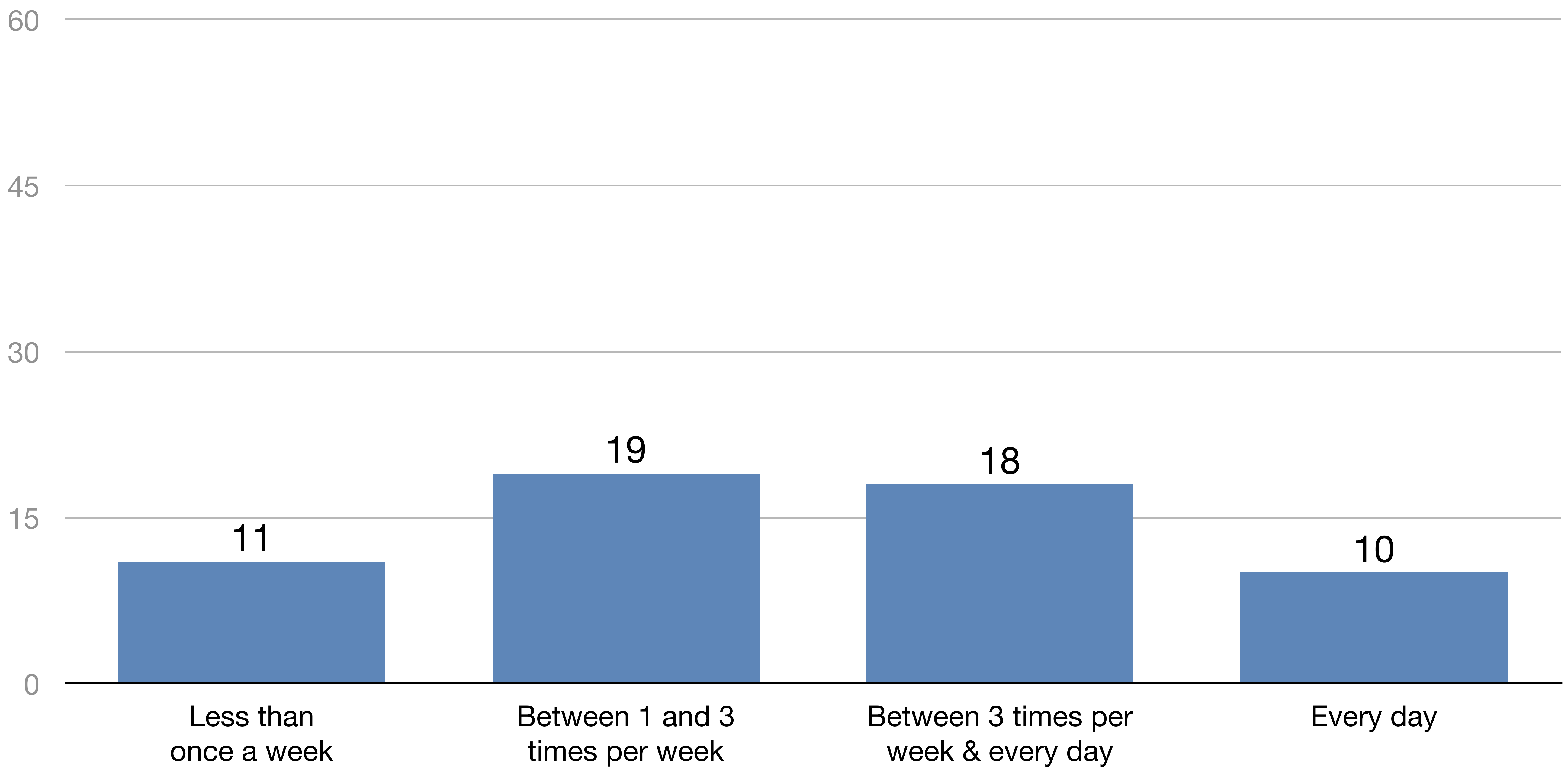
Prior experience with MISP



N=74

Participants

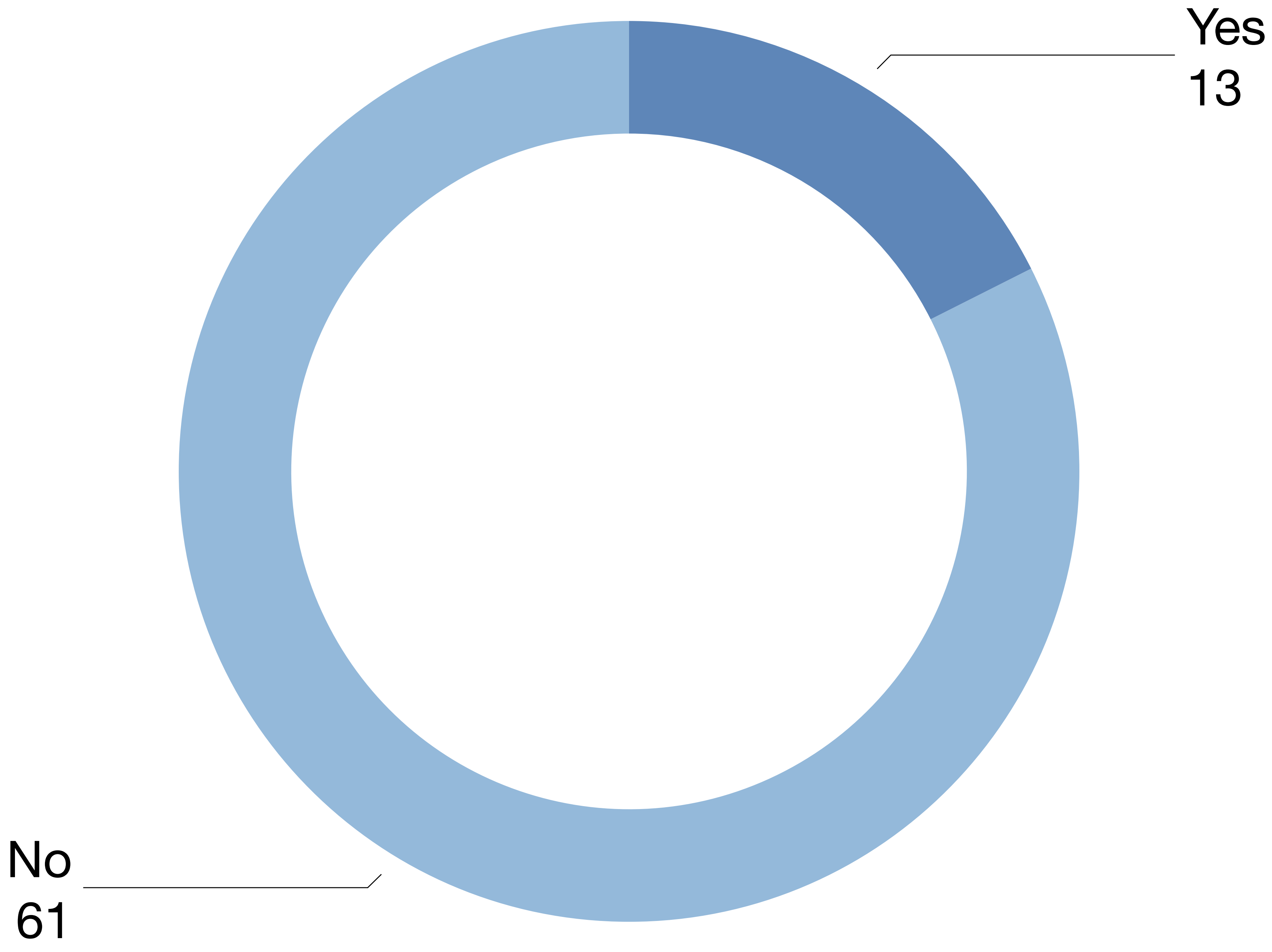
MISP usage frequency



N=52

Participants

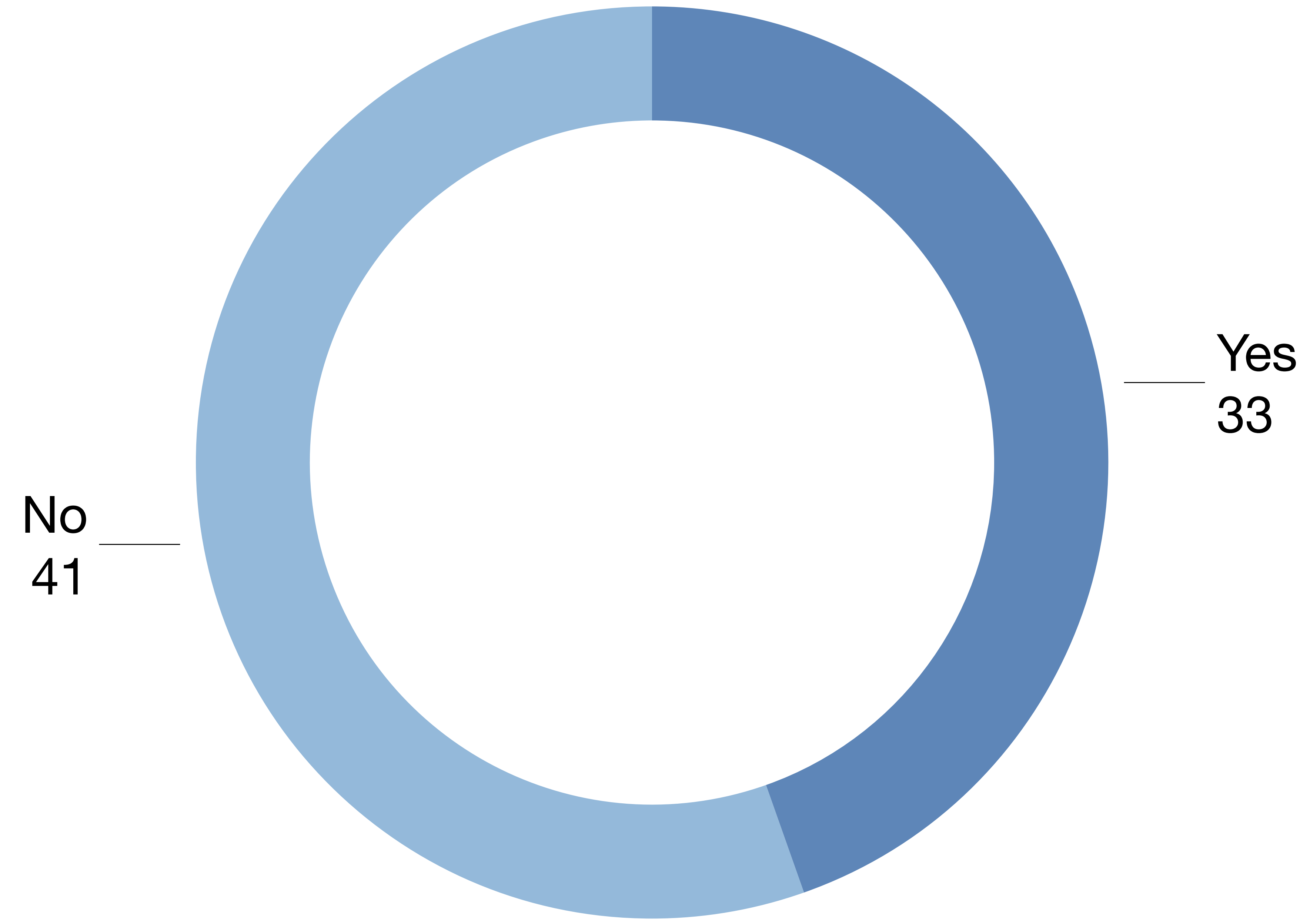
Previously attended a MISP training



N=74

Participants

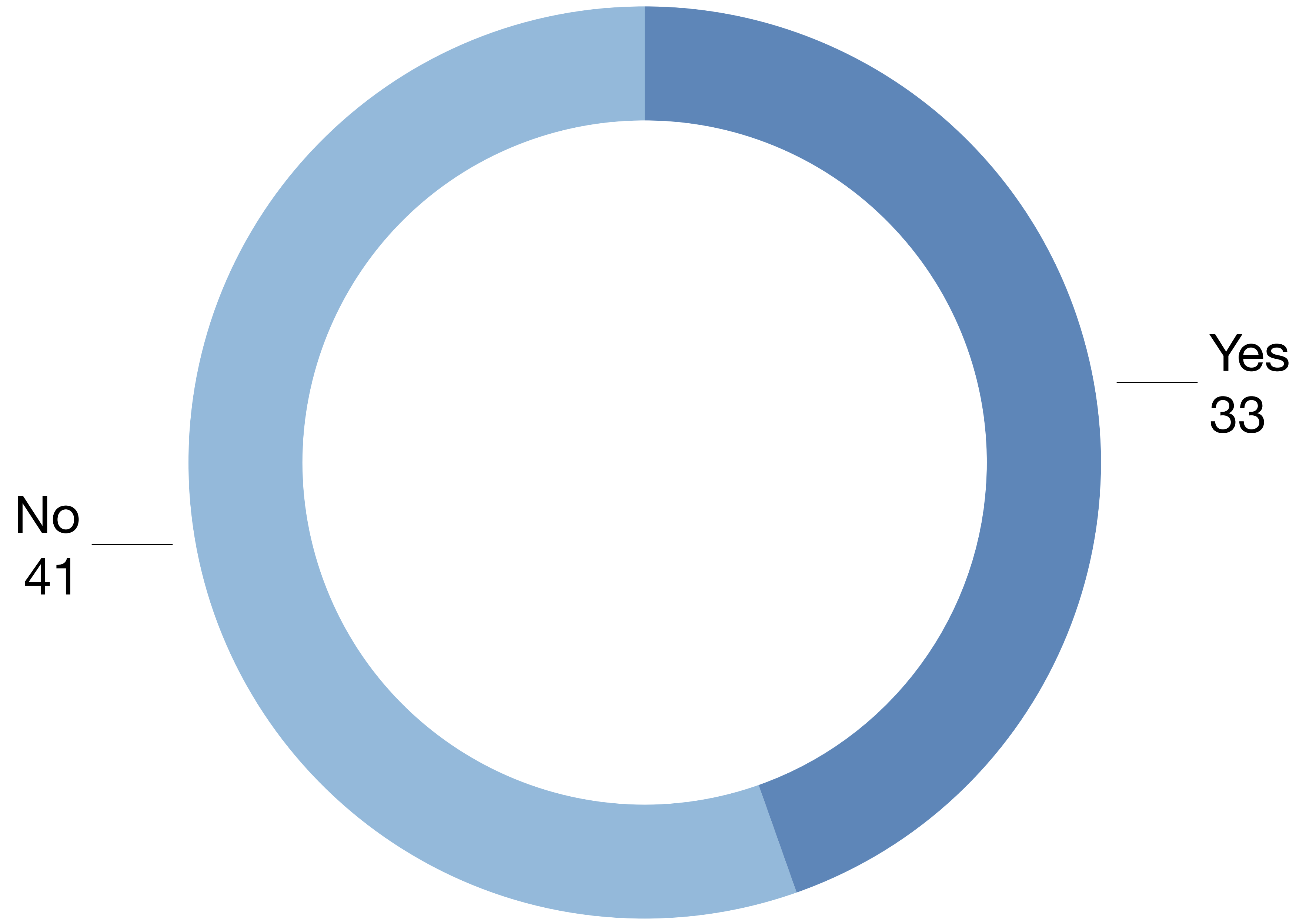
Previously used MISP training materials



N=74

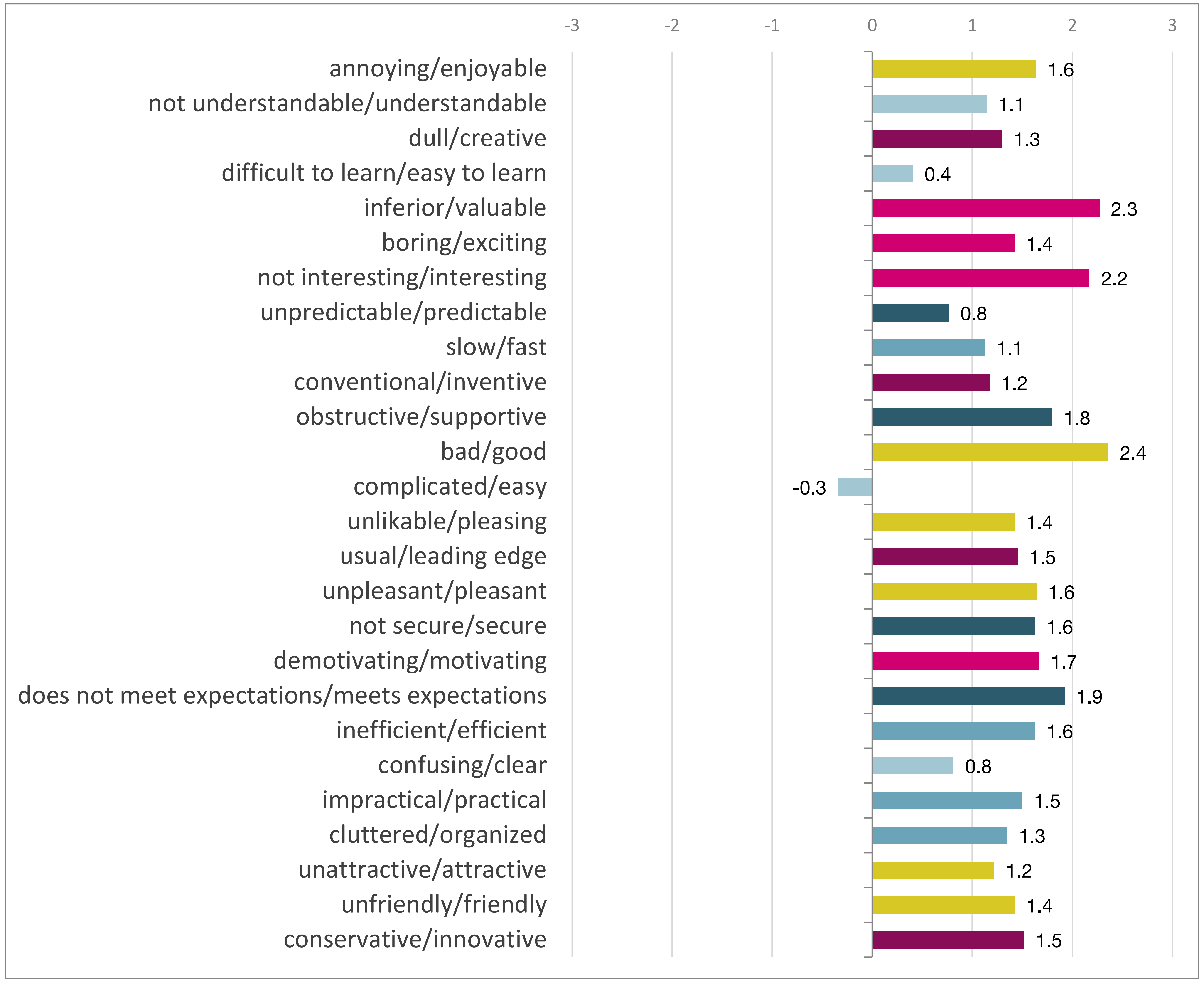
Participants

Previously used MISP virtual machines



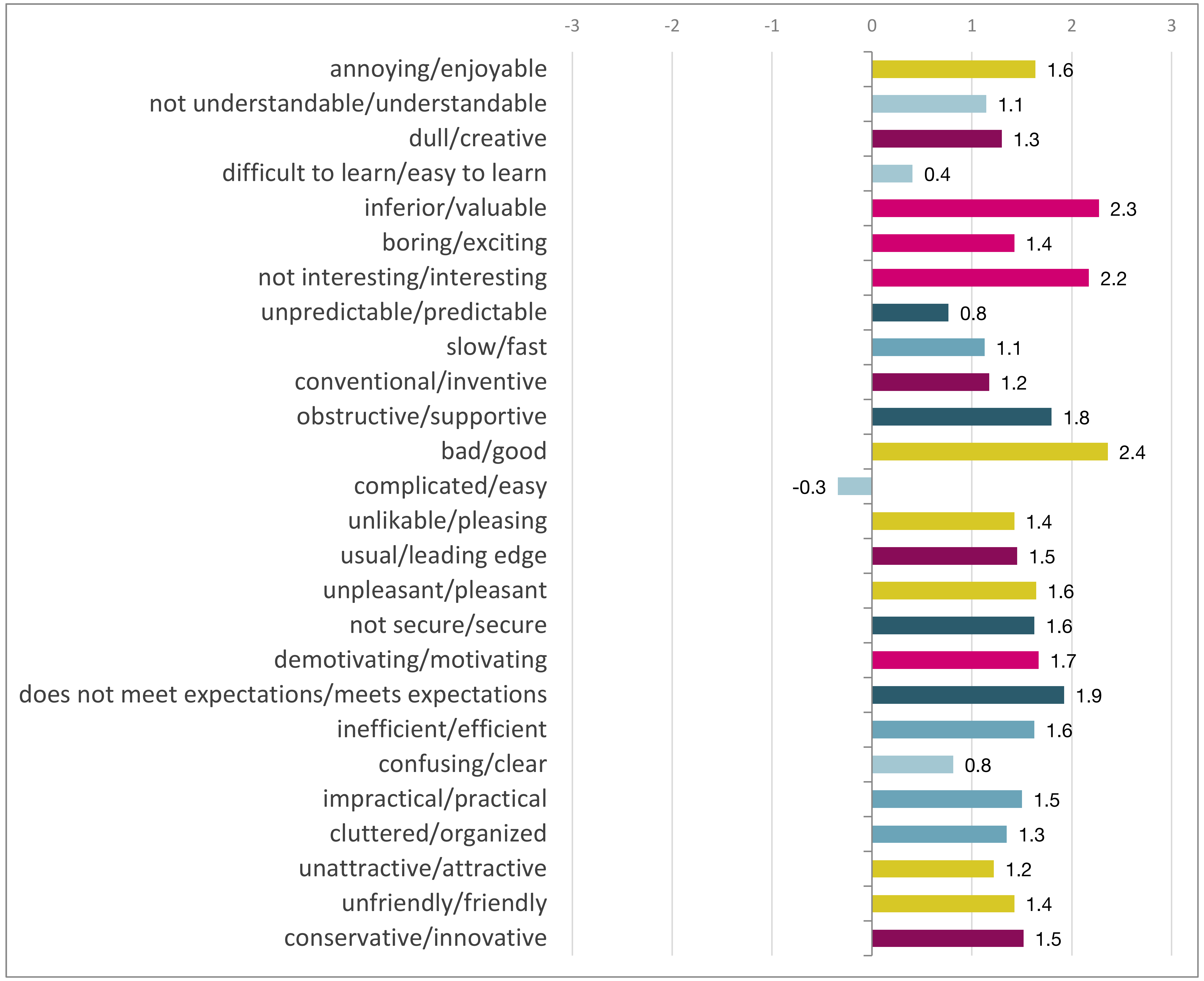
N=74

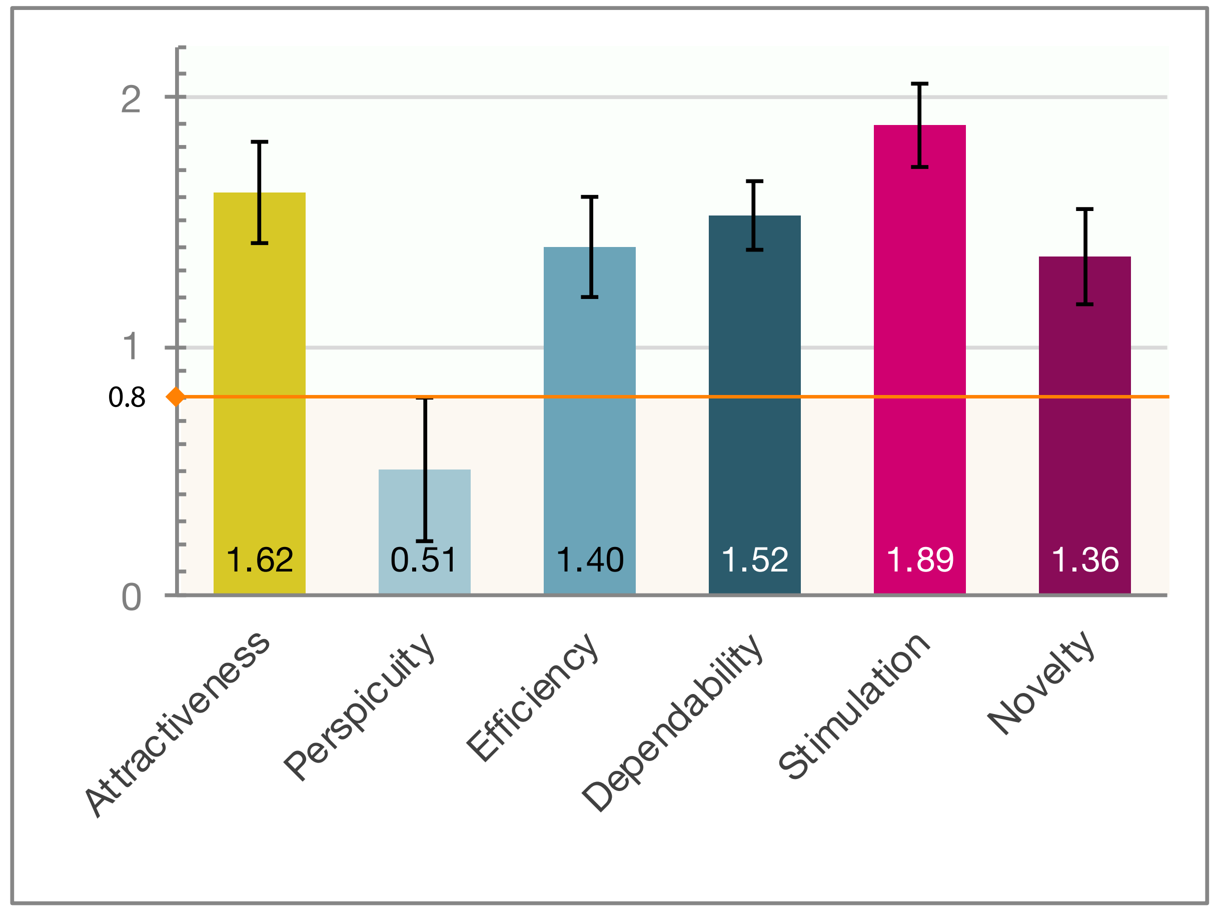
UEQ Results

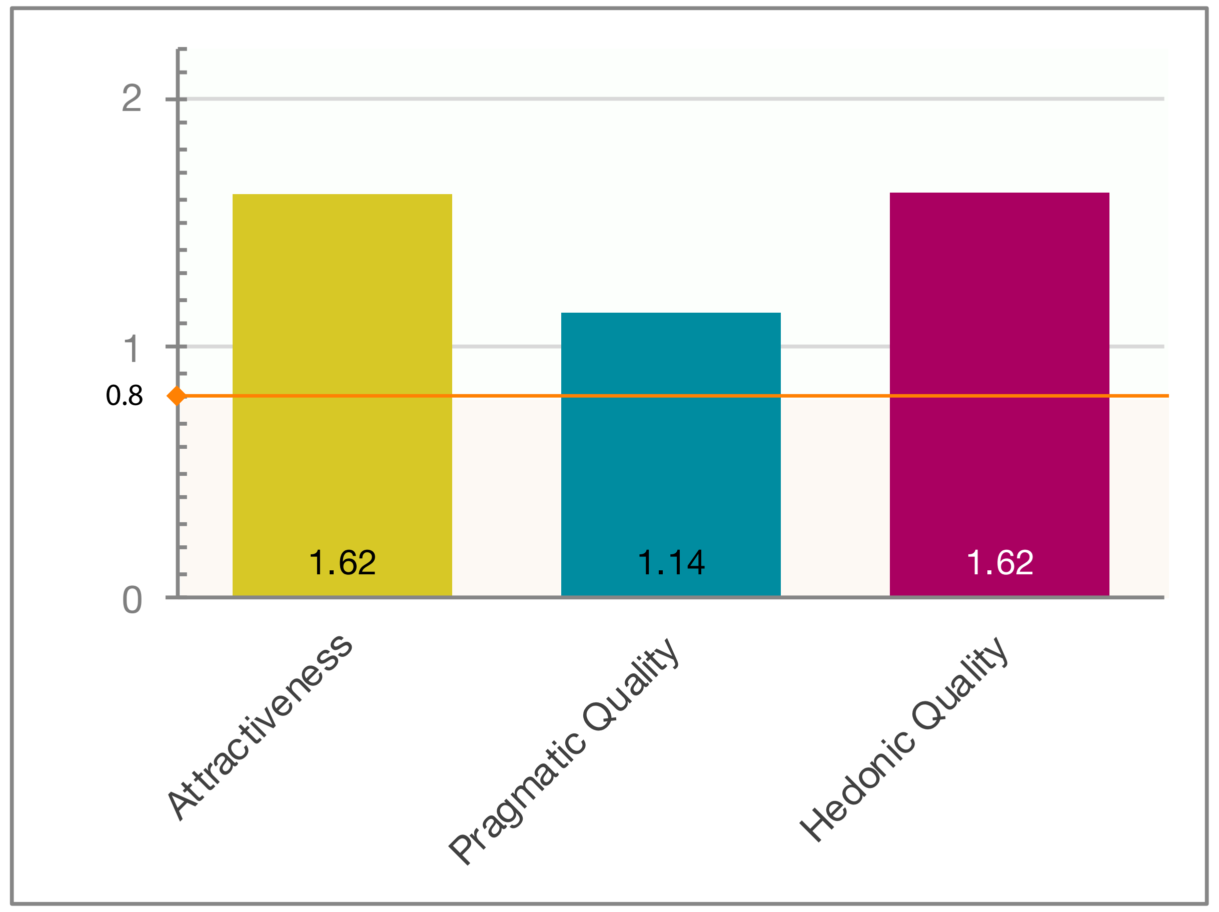


N=64

UEQ Results

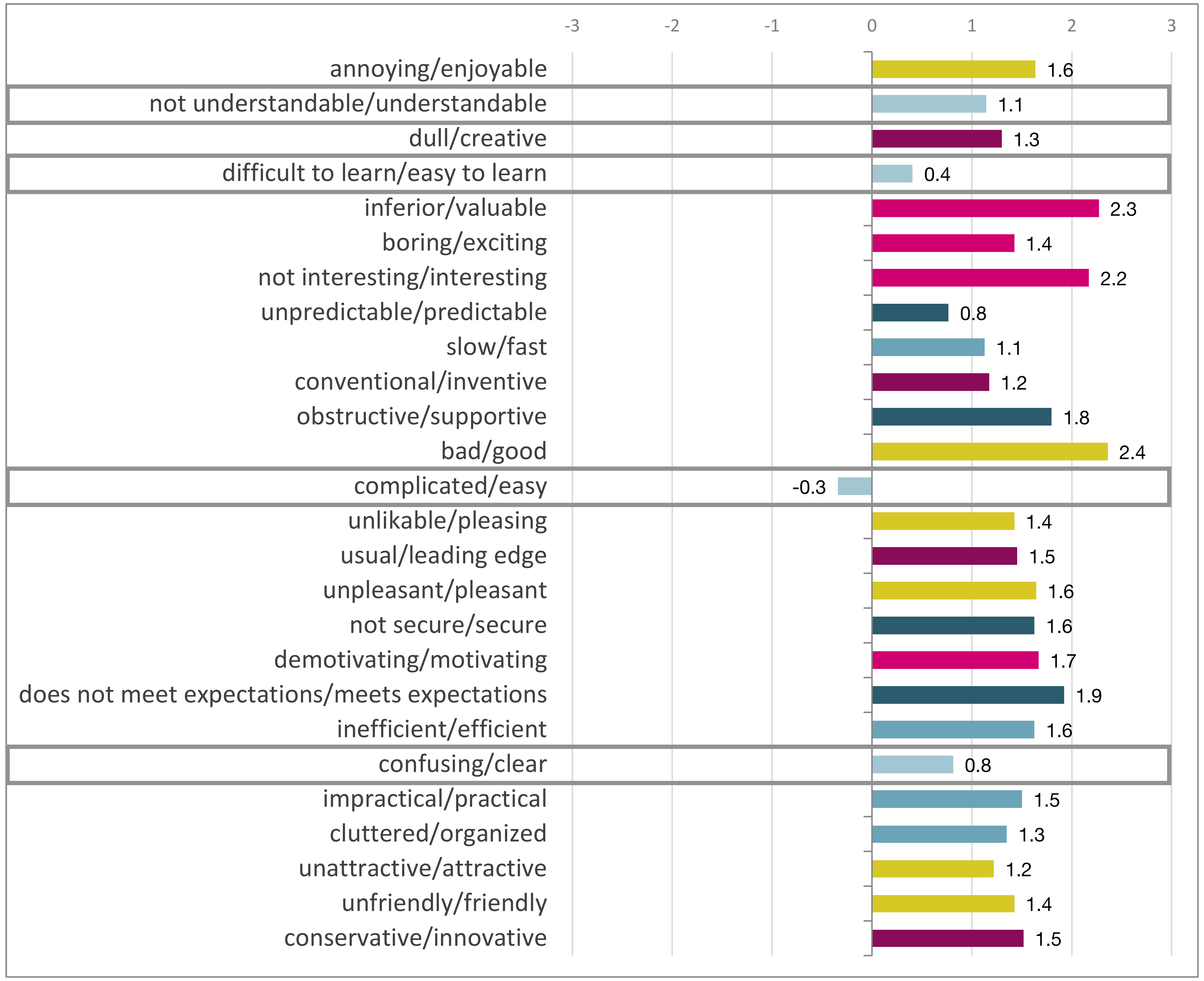


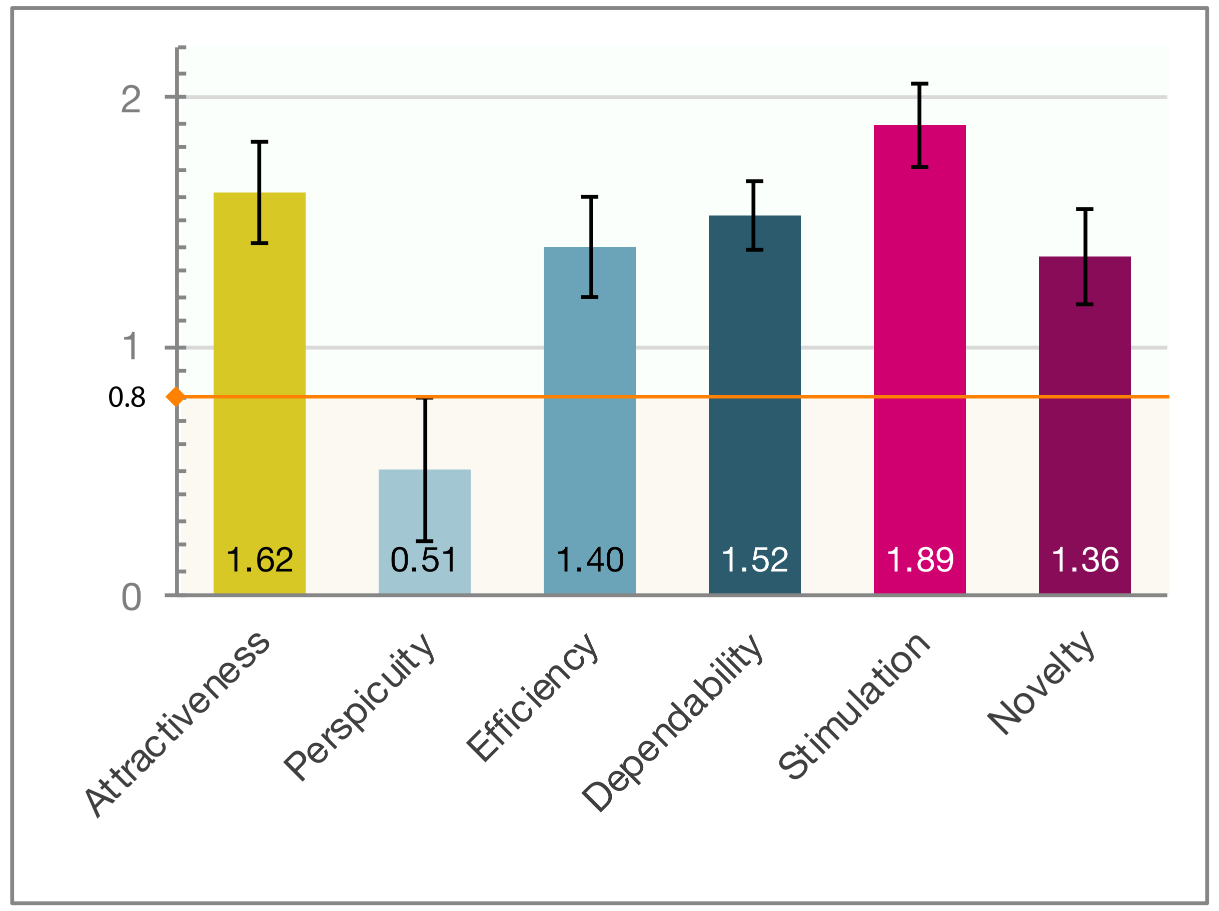


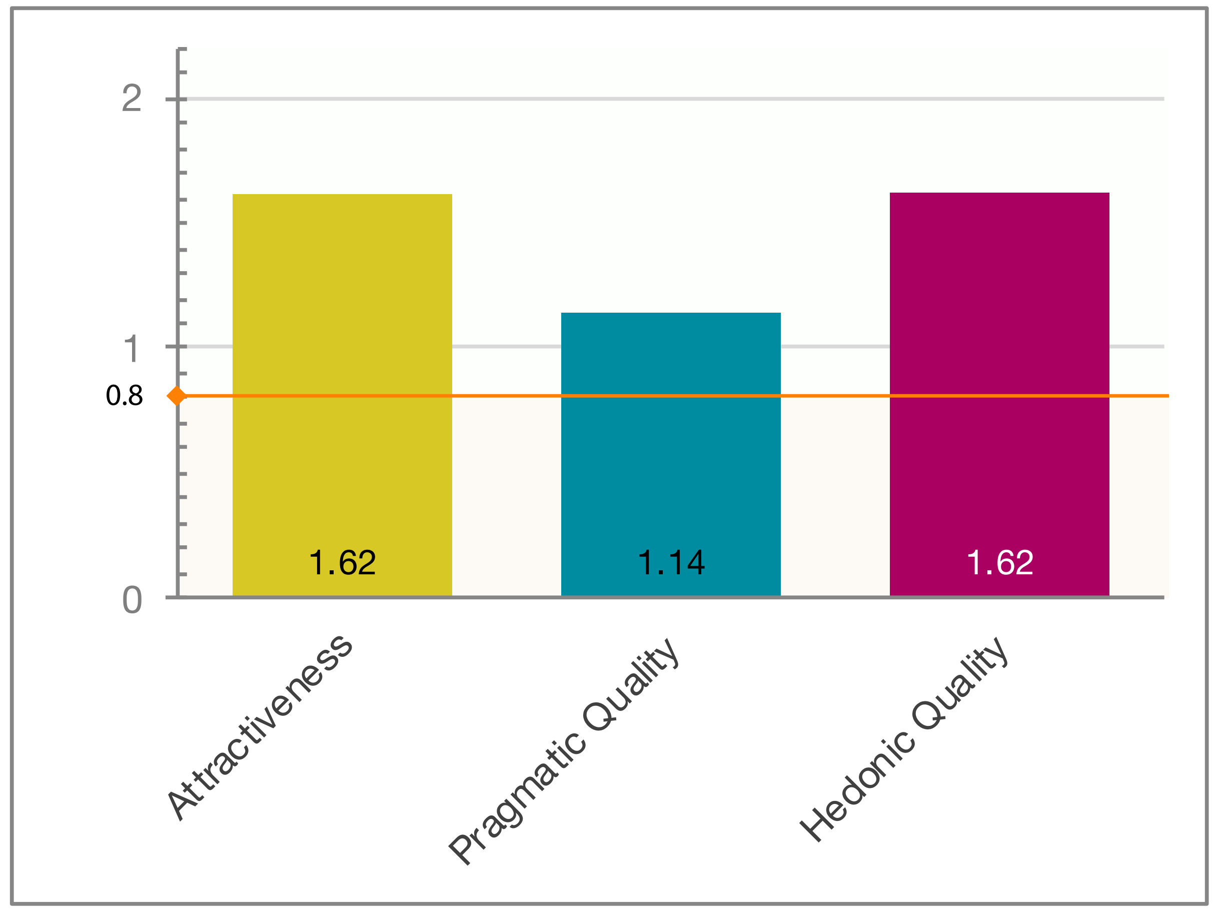


N=64

UEQ Results



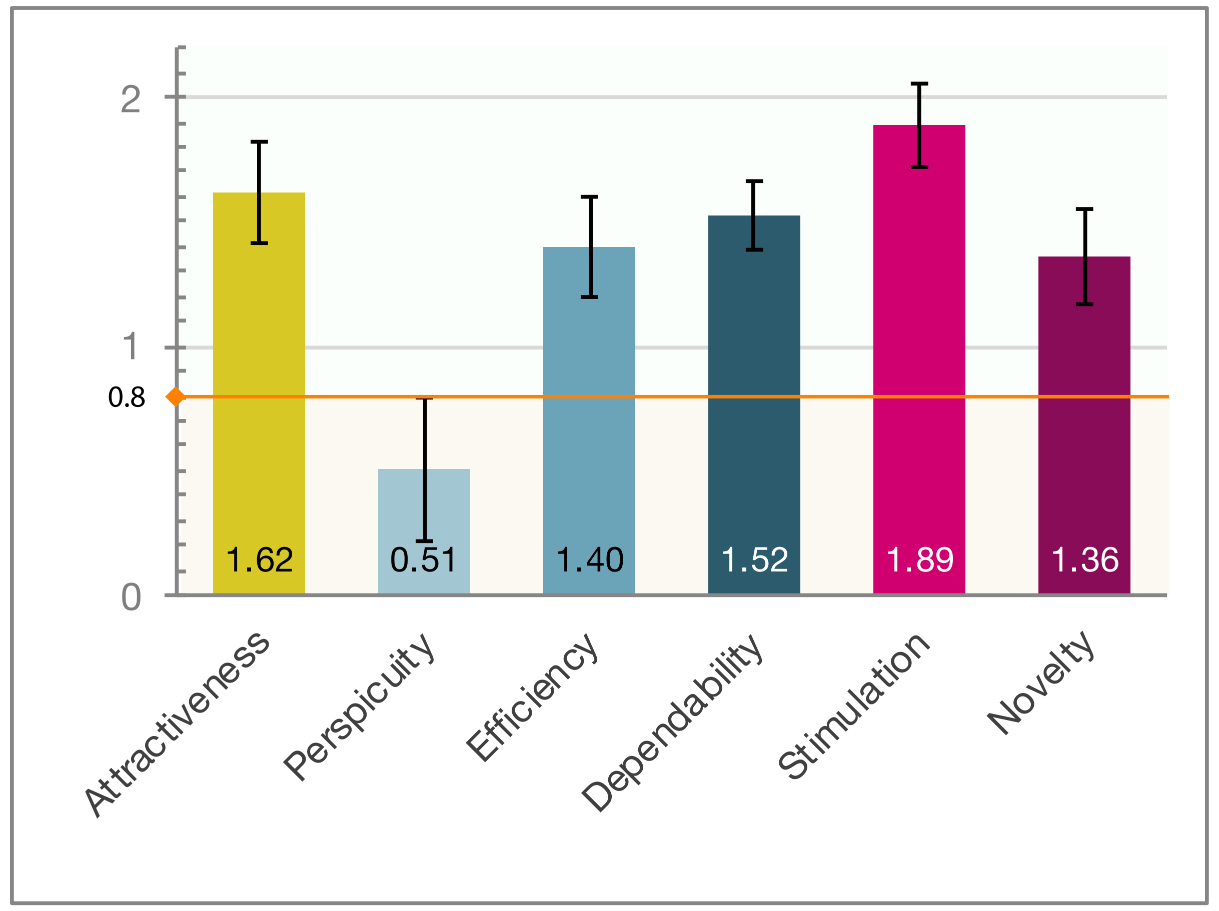




N=64

UEQ Results

Scale	Evaluation	Mean	Std Dev.	MoE	5% CI
Attractiveness	↗ Positive	1.62	0.83	0.203	[1.41, 1.82]
Perspicuity	→ Neutral	0.51	1.18	0.288	[0.21, 0.79]
Efficiency	↗ Positive	1.40	0.82	0.201	[1.20, 1.60]
Dependability	↗ Positive	1.52	0.56	0.138	[1.39, 1.66]
Stimulation	↗ Positive	1.89	0.68	0.167	[1.72, 2.05]
Novelty	↗ Positive	1.36	0.78	1.191	[1.17, 1.55]



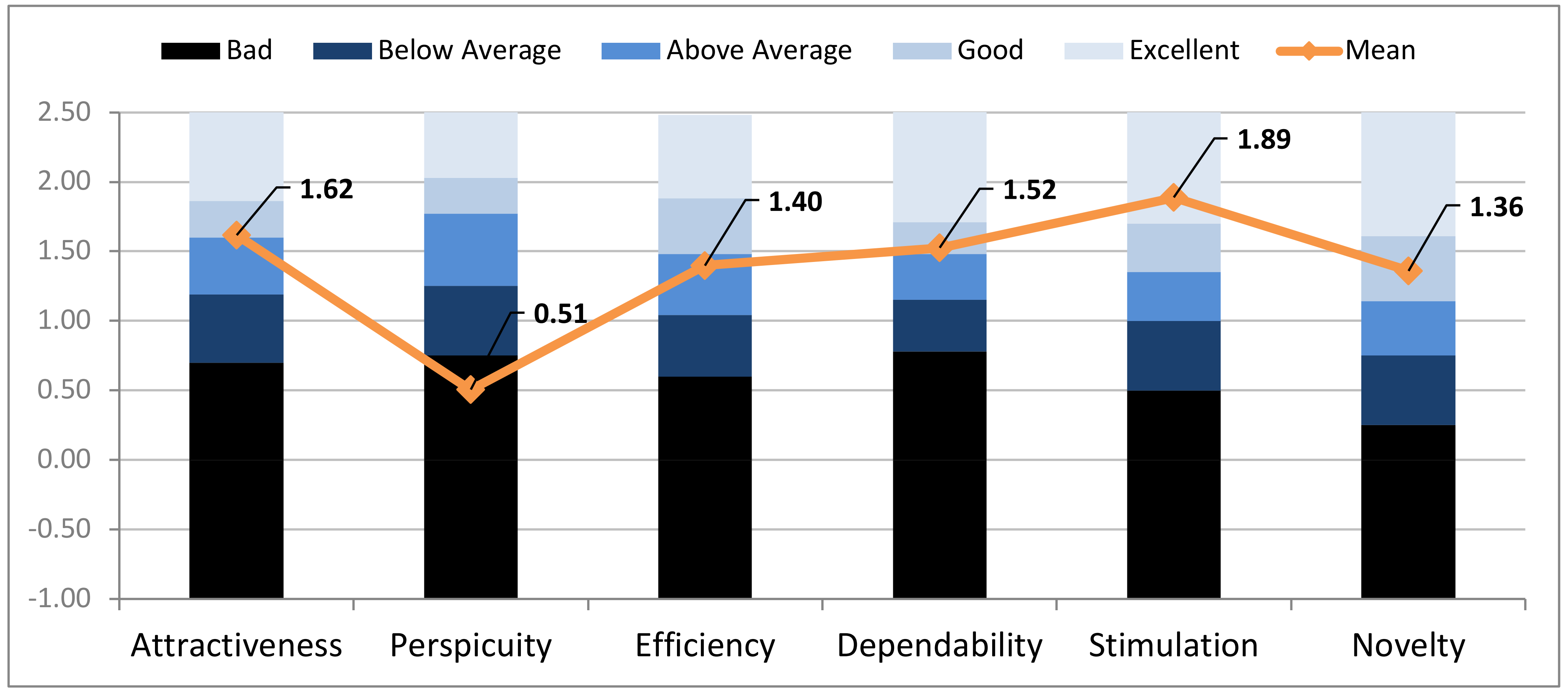
N=64

UEQ Results

Comparison of the MISP results to a general UEQ benchmark

(452 product evaluations)

Scale	Mean	Comparison	Interpretation
Attractiveness	1.62	Good	10% of results better, 75% of results worse
Perspicuity	0.51	Bad	In the range of the 25% worst results
Efficiency	1.40	Above average	25% of results better, 50% of results worse
Dependability	1.52	Good	10% of results better, 75% of results worse
Stimulation	1.89	Excellent	In the range of the 10% best results
Novelty	1.36	Good	10% of results better, 75% of results worse

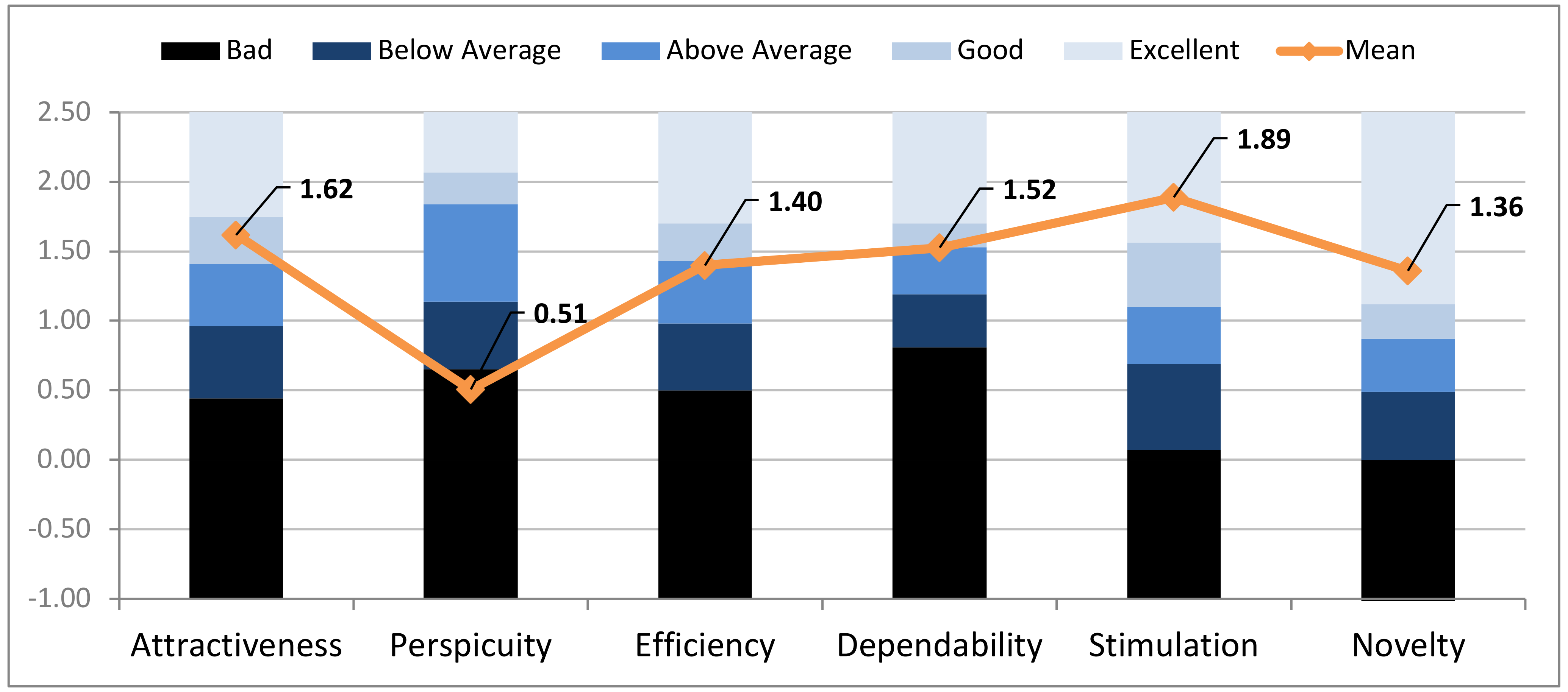


UEQ Results

Comparison of the MISP results to a UEQ benchmark of websites and web services

(85 product evaluations)

Scale	Mean	Comparison	Interpretation
Attractiveness	1.62	Good	10% of results better, 75% of results worse
Perspicuity	0.51	Bad	In the range of the 25% worst results
Efficiency	1.40	Above average	25% of results better, 50% of results worse
Dependability	1.52	Above average	25% of results better, 50% of results worse
Stimulation	1.89	Excellent	In the range of the 10% best results
Novelty	1.36	Excellent	In the range of the 10% best results



SC Results

Overview of Sentence completion stems and corresponding response rates

Sentence stems	Responses	No answer
S1: *When I use MISP, I feel …*	29 (69%)	13 (31%)
S2: *MISP is best for …*	29 (69%)	13 (31%)
S3: *MISP is not suitable for …*	19 (45%)	23 (55%)
S4: *I think the appearance of MISP is …*	31 (74%)	11 (26%)
S5: *I am happy with MISP because …*	32 (76%)	10 (24%)
S6: *The problem with MISP is …*	27 (64%)	15 (36%)
S7: *People who use MISP are typically …*	20 (48%)	22 (52%)
S8: *Compared to other threat information sharing platforms, MISP is …*	24 (57%)	18 (43%)
Total:	**211 (63%)**	**125 (37%)**

N=42

SC Results

Overview of most frequent themes (1/2)

Themes	**Theme frequency per sentence stem**								
	S1	S2	S3	S4	S5	S6	S7	S8	Total
User-related aspects									
Needs and values	9	0	0	0	11	2	4	6	**32**
Emotion evocation	34	2	0	4	1	3	0	0	**44**
- *Positive emotions*	*22*	*2*	*0*	*0*	*0*	*2*	*0*	*0*	*26*
- *Negative emotions*	*12*	*0*	*0*	*4*	*1*	*1*	*0*	*0*	*18*
User characteristics	0	1	7	1	0	6	13	0	**28**

SC Results

Overview of most frequent themes (2/2)

Themes	Theme frequency per sentence stem								
	S1	S2	S3	S4	S5	S6	S7	S8	Total
System-related aspects									
MISP characteristics	1	0	0	0	12	6	1	7	**27**
UX qualities	16	34	12	39	31	25	2	21	**180**
- *Attractiveness*	*0*	*0*	*0*	*16*	*0*	*0*	*0*	*6*	*22*
- *Lack of attractiveness*	*0*	*0*	*0*	*5*	*0*	*2*	*0*	*0*	*7*
- *Pragmatic qualities*	*3*	*34*	*0*	*7*	*29*	*0*	*2*	*10*	*85*
- *Lack of pragmatic qualities*	*10*	*0*	*12*	*7*	*0*	*23*	*0*	*0*	*52*
- *Hedonic qualities*	*3*	*0*	*0*	*0*	*2*	*0*	*0*	*5*	*10*
- *Lack of hedonic qualities*	*0*	*0*	*0*	*4*	*0*	*0*	*0*	*0*	*4*

User-related aspects

Needs and values: competence, control, autonomy, relatedness/belongingness

S1 *“When I use MISP, I feel confident about my ability to find bad guys”* (BM11)

S5 *“ I am happy with MISP because its flexibility allows me to solve my problems and I do not have to change my way of working”* (BM18)

S1 *“When I use MISP, I feel I’m part of a community”* (LT19)

S5 *“ I am happy with MISP because I’m a part of a community, I can help people like me”* (BM9)

User-related aspects

Evocation of positive emotions: satisfaction, confidence, pride, courage

S1 *“When I use MISP, I feel like a genius”* (LT16)

S2 *“MISP is best for people who aren’t afraid of digging through Github issues as a supplement [sic] to the documentation”* (BM14)

User-related aspects

Evocation of negative emotions: confusion, boredom, frustration

S1 *“When I use MISP, I feel overwhelmed with the amount and type of data”* (BM12)

S6 *“The problem with MISP is its integration, that is confusing for me”* (LT27)

S1 *“When I use MISP, I feel a bit lost, need to search a lot to find what I need”* (BM7)

User-related aspects

Profile and characteristics of MISP users

S7 *"People who use MISP are typically experts on security"* (LT11)

S3 *"MISP is not suitable for non techies"* (BM11)

S3 *"MISP is not suitable for quick ad-hoc analysis by non IT professionals"* (LT25)

S6 *"The problem with MISP is a lack of a public community that new users can join when starting out"* (LT3)

System-related aspects

MISP characteristics: freeness, openness, adaptation

S5 *“I am happy with MISP because it has potential to integrate with other tools and is open-source”* (LT16)

S8 *“Compared to other threat intelligence sharing platforms, MISP is free, open-source and not managed by big companies”* (BM20)

S5 *“I am happy with MISP because it just works 95% of the time and it’s enormously flexible as a tool”* (BM14)

S5 *“I am happy with MISP because it can be used in different ways”* (LT31)

System-related aspects

UX qualities: Attractiveness and lack thereof

S4 *“I think the appearance of MISP is quite pleasing”* (BM7)

S4 *“I think the appearance of MISP is very good”* (LT27)

S4 *“I think the appearance of MISP [is] has room for improvement”* (BM18)

S6 *“The problem with MISP is [its] look and feel”* (LT19)

System-related aspects

UX qualities: Pragmatic aspects

S8 *"Compared to other threat intelligence sharing platforms, MISP is well-maintained and good feature set"* (LT16)

S2 *"MISP is best for identifying events, their sources, and their attributes"* (LT7)

S2 *"... best for documenting malware and incidents and sharing that information"* (LT12)

S2 *"... best for having a centralized place to store and collaborate on data"* (LT19)

System-related aspects

UX qualities: Pragmatic issues

S6 *“The problem with MISP is it is too IOC-centered / IOC-oriented”* (BM2)

S3 *“MISP is not suitable for long term analysis or assessment”* (LT13)

S4 *“I think the appearance of MISP is chaotic at times”* (BM6)

S6 *“The problem with MISP is finding the balance between good enough information and time invested”* (LT12)

System-related aspects

UX qualities: Pragmatic issues

S6 *“The problem with MISP is that it is huge and kind of hard to start with”* (LT11)

S6 *“The problem with MISP is it has a steep learning curve”* (LT16)

S4 *“I think the appearance of MISP needs to be explained to be more used”* (LT28)

S6 *“The problem with MISP is it is hard to get started adding events if you never saw an example”* (LT6)

System-related aspects

UX qualities: Hedonic aspects

S4 *“I think the appearance of MISP is good, but a little old fashioned”* (BM9)

S8 *“Compared to other threat intelligence sharing platforms, MISP is a breath of fresh air”* (BM14)

S4 *“I am happy with MISP because it is an awesome tool”* (LT27)

4 Discussion and Future Work

Summary of key findings

- Overall positive UX evaluation across the three main system quality aspects: **attractiveness, pragmatic** and **hedonic qualities**
  - Lower *pragmatic* evaluation due to low *perspicuity* score
- Complex relationship users have with MISP:
  - **useful**, **valuable**, and **empowering**, but also overwhelming
  - flexibility, adaptation, openness, community

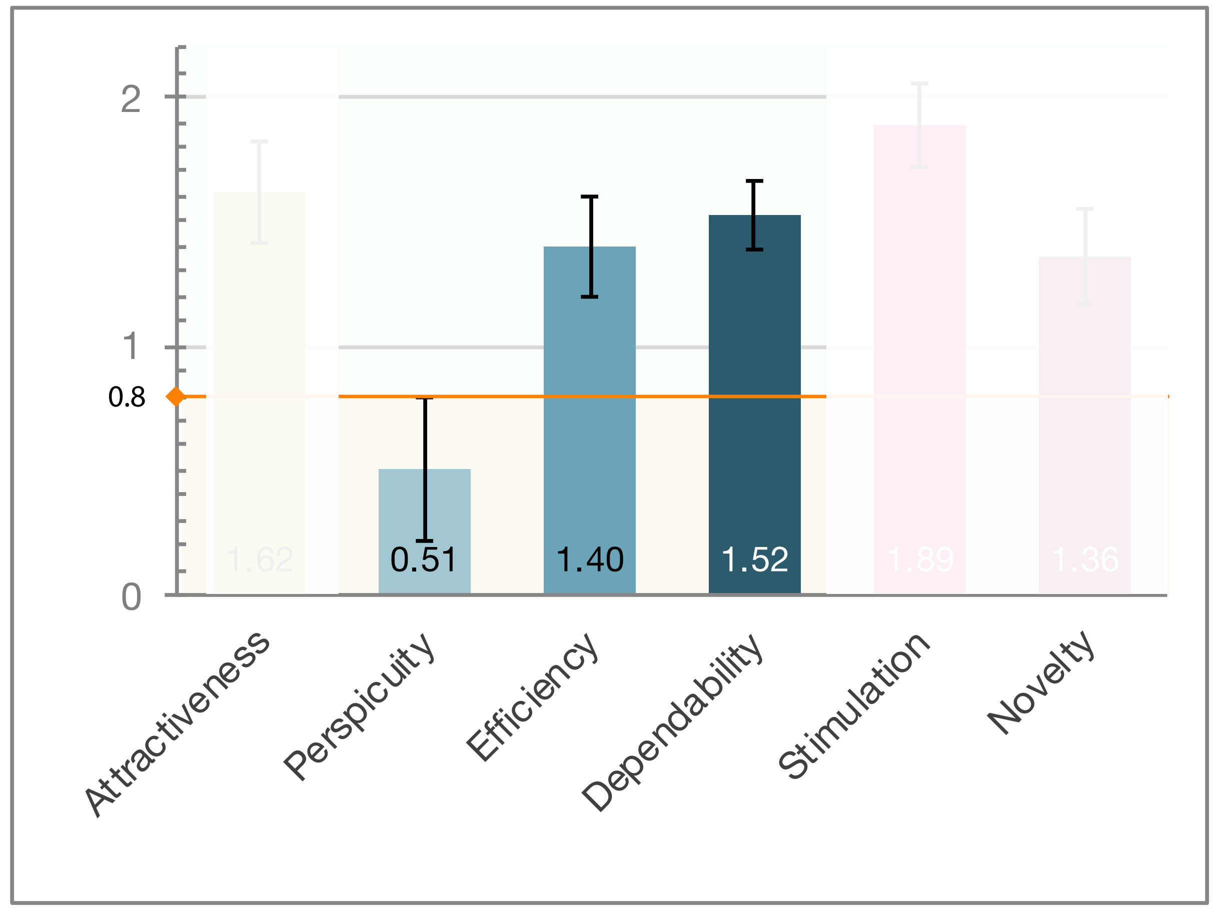
Implications

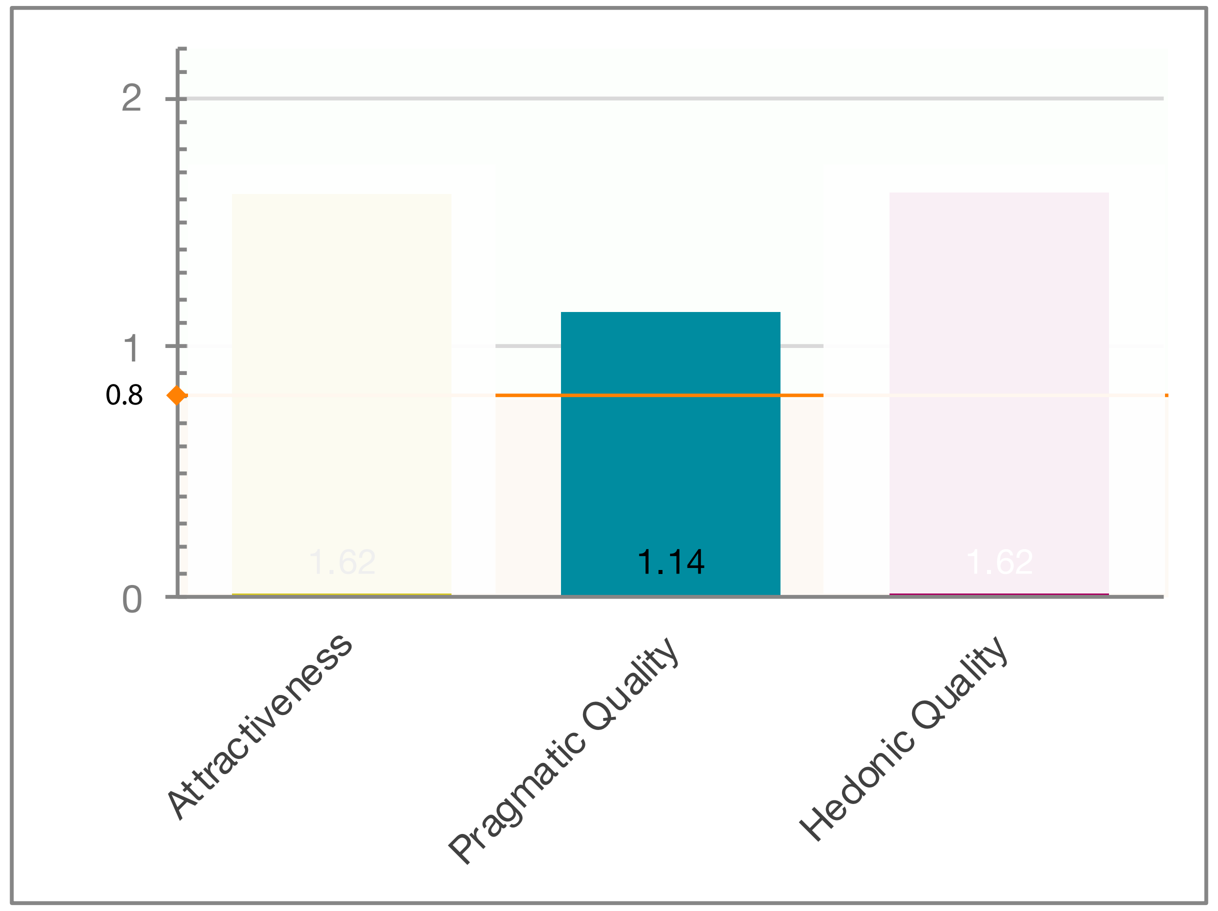
- Highlighted concerns open potential problems in terms of **errors** and **under-utilization**
  - people have nuanced behavior with respect to *how*, *with whom*, *when*, and *why* they share sensitive information
- Sharing without knowing who the (intended) recipients are, can lead to:
  - **oversharing** i.e. leakage of sensitive information to parties beyond those intended
  - **undersharing** i.e. lower cyber preparedness levels of the sharing community
  - both impact the future use and adoption, where no adoption means lower security

Beyond usability

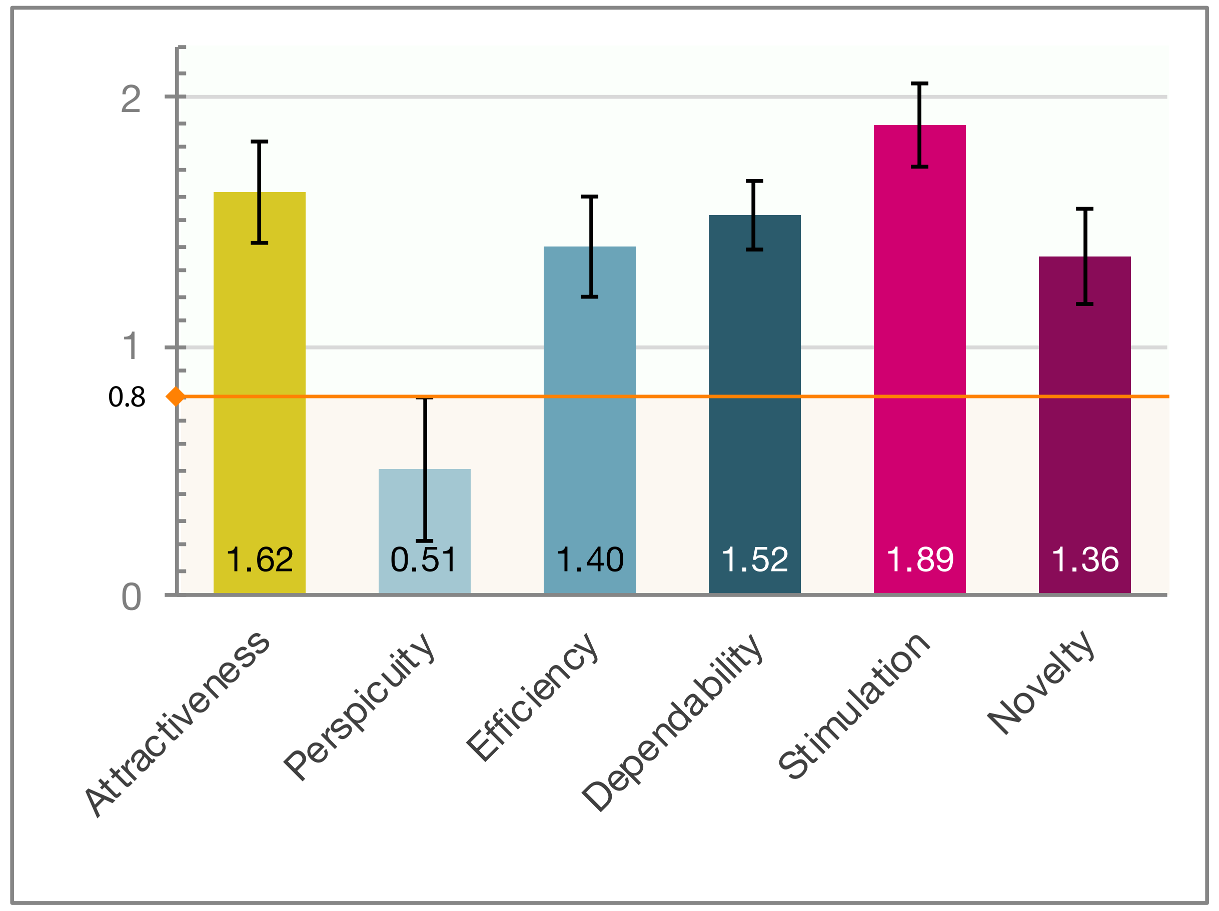
- **Why start/continue using a CTI platform even though it is hard to learn?**
  - Narrow usability-focused studies focus on task-related efficiency and effectiveness, but omit other equally important aspects

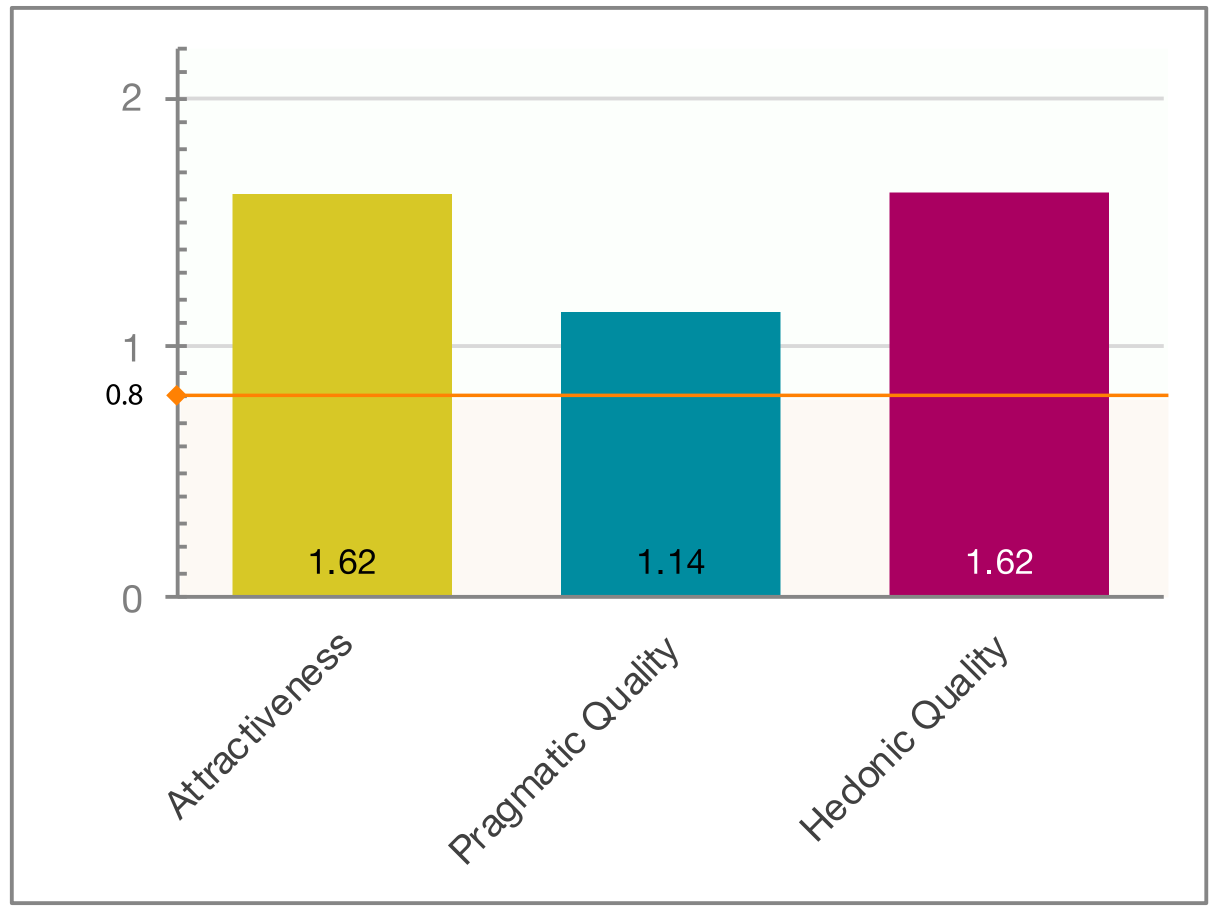
UEQ Results





versus





Beyond usability

- **Why start/continue using a CTI platform even though it is hard to learn?**
  - Narrow usability-focused studies focus on task-related efficiency and effectiveness, but omit other equally important aspects
- Affective reactions before, during, or after use, emotional relationships people build with products, fulfillment of phycological needs
  - Psychological need of **relatedness** / **belongingness** can play a key role here
- Importance of approaching UX in a holistic manner

Limitations

- Difficulties recruiting and getting access to larger numbers of participants
    - Sample skewed towards novice users, mostly male, with a tech background
    - Study period of two years, not exactly the same version of MISP, however, no radical changes introduced w.r.t. activities covered during MISP training sessions
- Limitations of deployed methods, as every context is specific and the methods are not a perfect fit for every situation

Future Work

- Further validation of obtained results and assumptions e.g. impact of expertise and experience with the platform on the evaluation
- More research on UX aspects and how UX design can help
    - Do users have a correct understanding of how far CTI information travels when shared?
    - How are users supported in core activities (e.g. UI mechanisms, docs, training)?
    - How does end-user feedback loop back to the designers and developers and whose responsibility is the UX in open-source, community-driven projects like MISP?

Conclusion

- CTI exchange is a crucial element in the fight against increasing cyber attacks and threats
- Through the use case of MISP, we have highlighted what novice users perceive to be the strengths and weaknesses of a leading CTI sharing platform
  - Specified appropriate metrics and performed a benchmark UX evaluation
- We demonstrated that many user and system-related needs can remain hidden unless we take an **expanded notion of the UX** and go beyond narrow usability studies

Thank you for your attention! Any questions?

Borče Stojkovski
SnT, University of Luxembourg

@b0rce

borce.stojkovski@uni.lu
94D2 ED64 1642 66E2