CURRENT CYBERSECURITY STATUS IN ROBOTICS :
INSIGHTS ON ROBOT SECURITY SURVEY
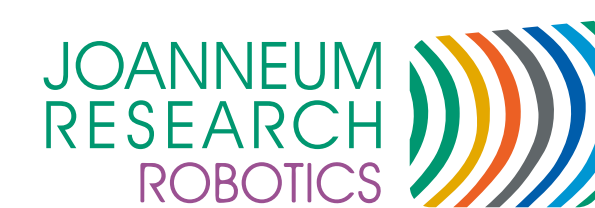
ALIAS ROBOTICS
Robot Cybersecurity

JOANNEUM
RESEARCH
ROBOTICS

ENDIKA GIL-URIARTE

CSO

endika@aliasrobotics.com

Endika Gil-Uriarte, Victor Mayoral Vilches, Oxel Urzelai, David Mayoral and Bernhard Dieber.

BACKGROUND

ROBOT SECURITY
SURVEY

ALIAS ROBOTICS
Robot Cybersecurity

JOANNEUM
RESEARCH
ROBOTICS

CONTEXT
Robotics is at its dawn. Cybersecurity is a novel "concern" at the advent of Industry 4.0

SEVERAL ROBOT TECHNOLOGIES
are hitting the market, such as ROS (Robot Operating System) as a "de facto" standard. But proprietary systems are still maintained.

SAFETY VS SECURITY IN ROBOTICS
Historically, focus in robotics has been put in ensuring safety. Security is not a main concern.

AWARENESS

We've found that most manufacturers are not caring about cybersecurity. Most robots are insecure by design.

BACKGROUND

ROBOT SECURITY
SURVEY

ALIAS ROBOTICS
Robot Cybersecurity

JOANNEUM RESEARCH ROBOTICS

(DISTINGUISHED) ROBOT MANUFACTURER QUOTES

"Security... yes, we hold PLD (and start safety pitch) blah"

"Cybersecurity flaws greatly facilitate system integration"

"We know our robots have a set of reported vulnerabilities"

"We leave solving those up to the end user"

"This is not hacking a robot... You are trying to drum up business to sell your consultancy services"

Upon Vulnerability advisory: "Do not connect your robot"

"Every thing will be fixed in the next release"... 3 months later... "It can't be fixed"

" Cybersecurity is up to the ~~robot~~ ~~user~~ hacker "

INTRODUCING
ROBOT SECURITY SURVEY

ROBOT SECURITY
SURVEY

ALIAS ROBOTICS
Robot Cybersecurity

JOANNEUM RESEARCH ROBOTICS
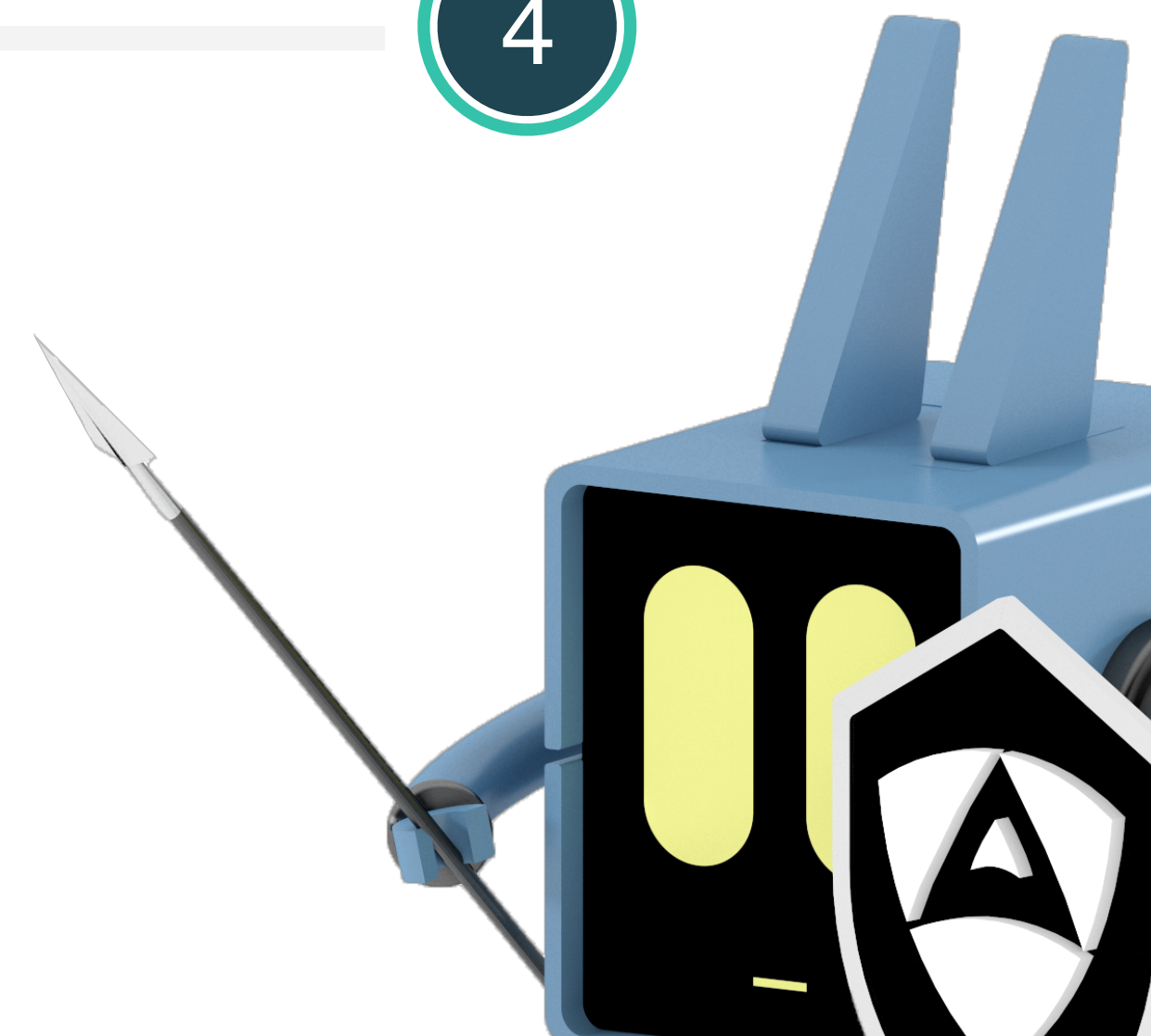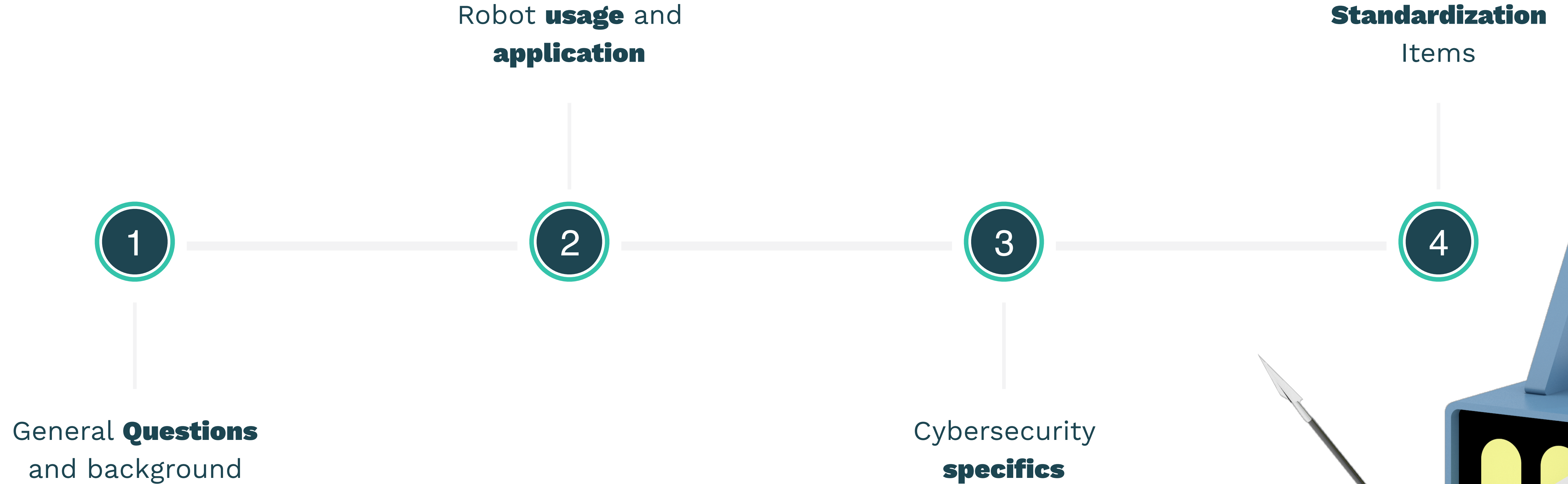
OBJECTIVE

Depict a global landscape of the current security situation in robotics.

RATIONALE

The need to assess precisely the security concerns of **the players** involved in the value chain and the strategies of cybersecurity so far.
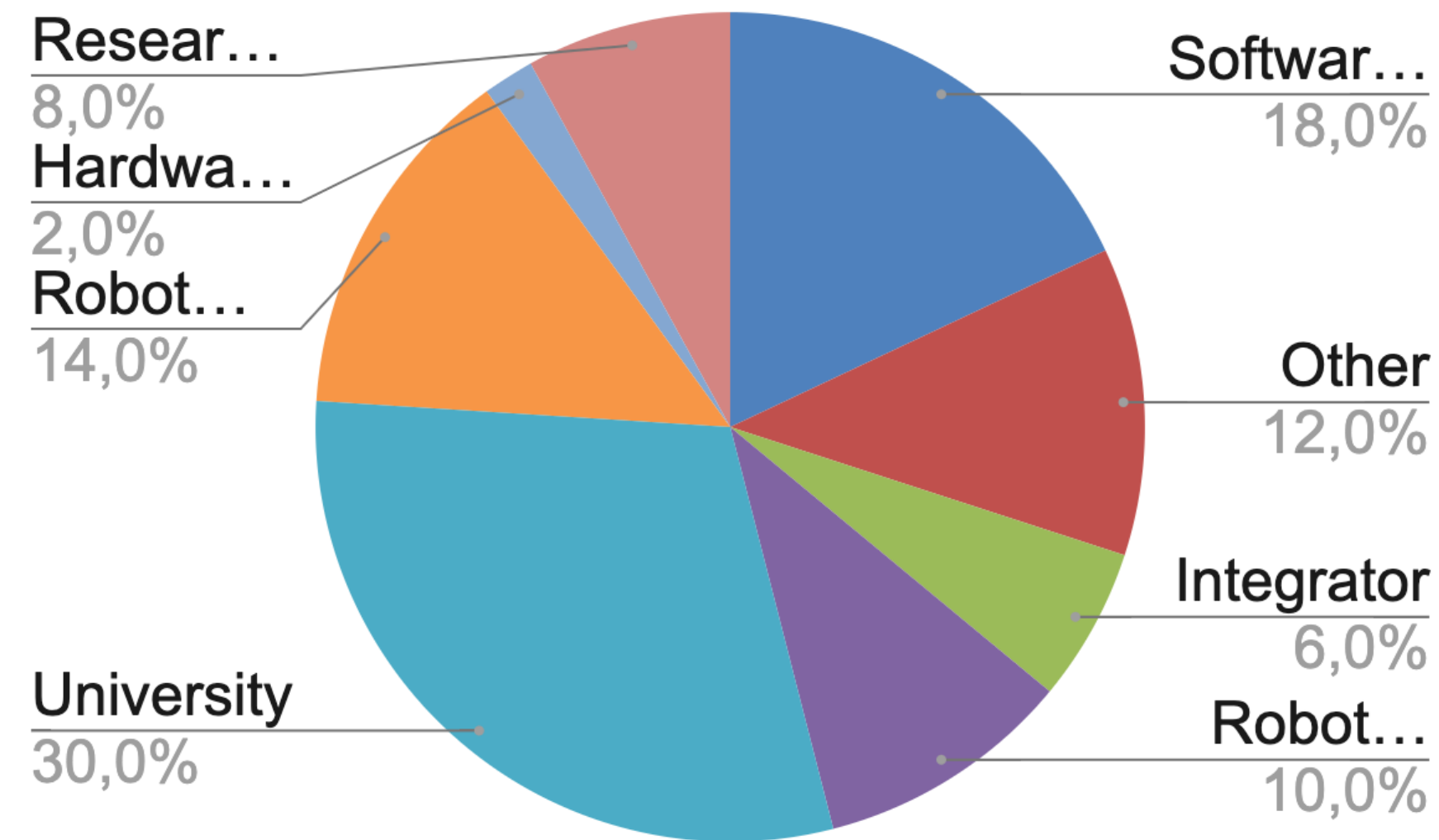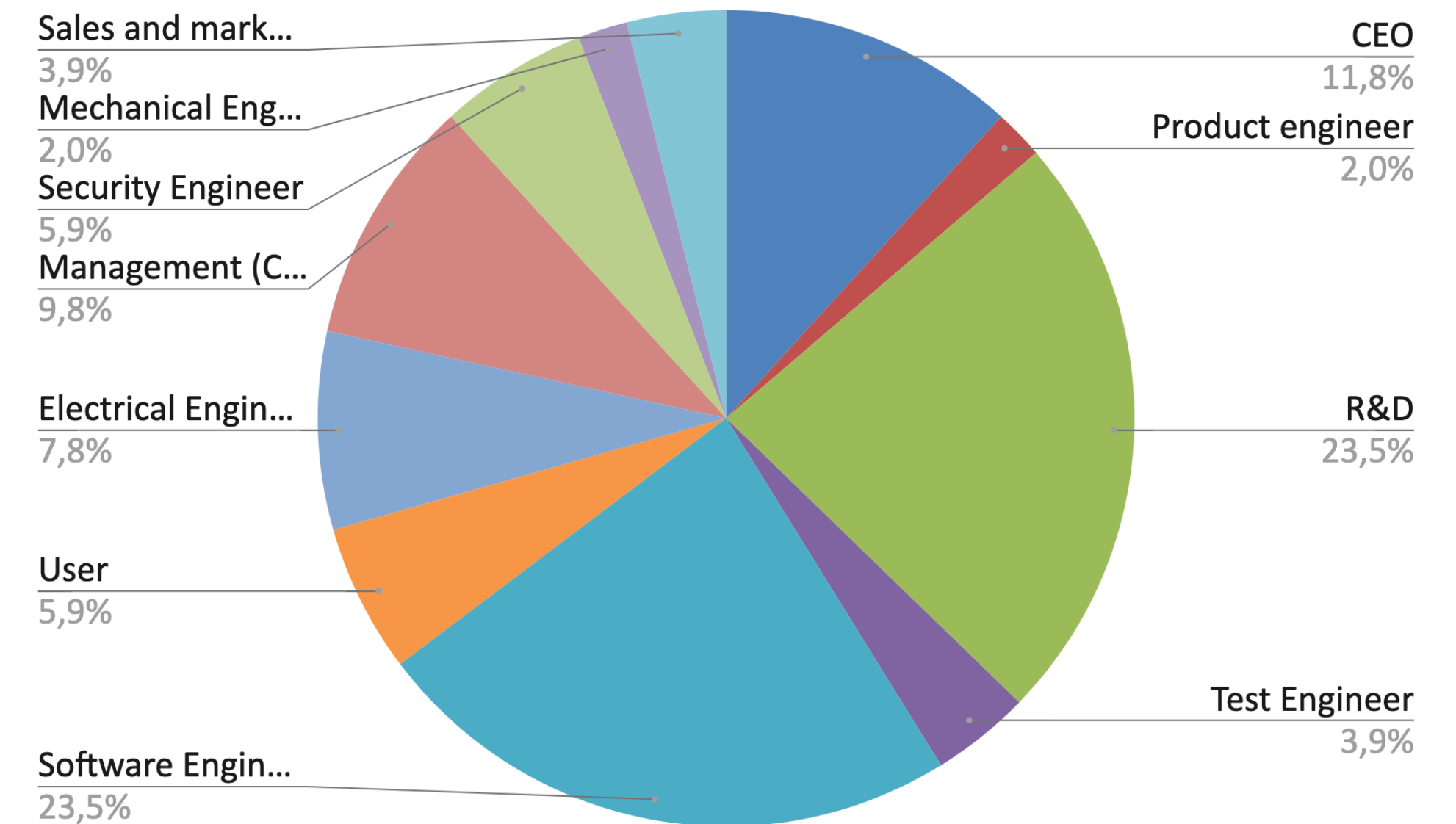
STRUCTURE
ROBOT SECURITY SURVEY

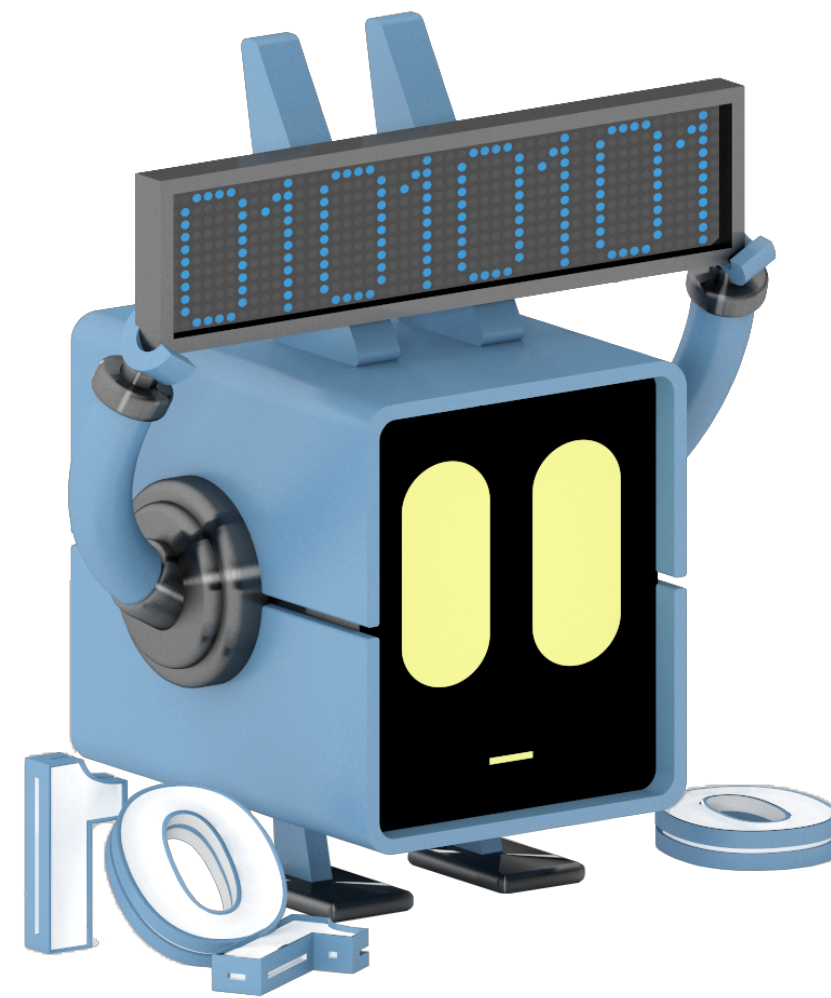Robot **usage** and **application**

Standardization Items

1

2

3

4

General **Questions** and background

Cybersecurity **specifics**

RESPONDANT PROFILES

51

RESPONDANT PROFILES

Softwar… 18,0%
Other 12,0%
Integrator 6,0%
Robot… 10,0%
University 30,0%
Robot… 14,0%
Hardwa… 2,0%
Resear… 8,0%

VARIOUS BACKGROUNDS & POSITIONS

CEO 11,8%
Product engineer 2,0%
R&D 23,5%
Test Engineer 3,9%
Software Engin… 23,5%
User 5,9%
Electrical Engin… 7,8%
Management (C… 9,8%
Security Engineer 5,9%
Mechanical Eng… 2,0%
Sales and mark… 3,9%

ROBOT
USAGE

59%

IMPROVED
EFFICIENCY,
REPEATABILITY
AND REPRODUCIBILITY

6.5

PERCEPTION
OF
USEFULNESS

4.4

RATING IN
TRANSPARENCY
& VISIBILITY

WORRIES

57%	They are erasing jobs
41%	Removing the human element from interaction
33,3%	Skynet-esque events
31,4%	Ethical accountability (Asimov's laws)
25,5%	They are a threat to physical safety
23,5%	They pose a cybersecurity risk

OPEN FRAMEWORK
USAGE

80%

::: ROS ::: 2

POPULARITY OF
OPEN SOURCE

100

75

50

25

0

ROS familiarity

Usefulness score

Activity rate

Discourse activity rate

STATS SPECIFIC
TO **ROS**

10

7,5

5

2,5

0

Security setup difficulty in ROS (1)

Security setup difficulty in ROS 2

Improved security perception
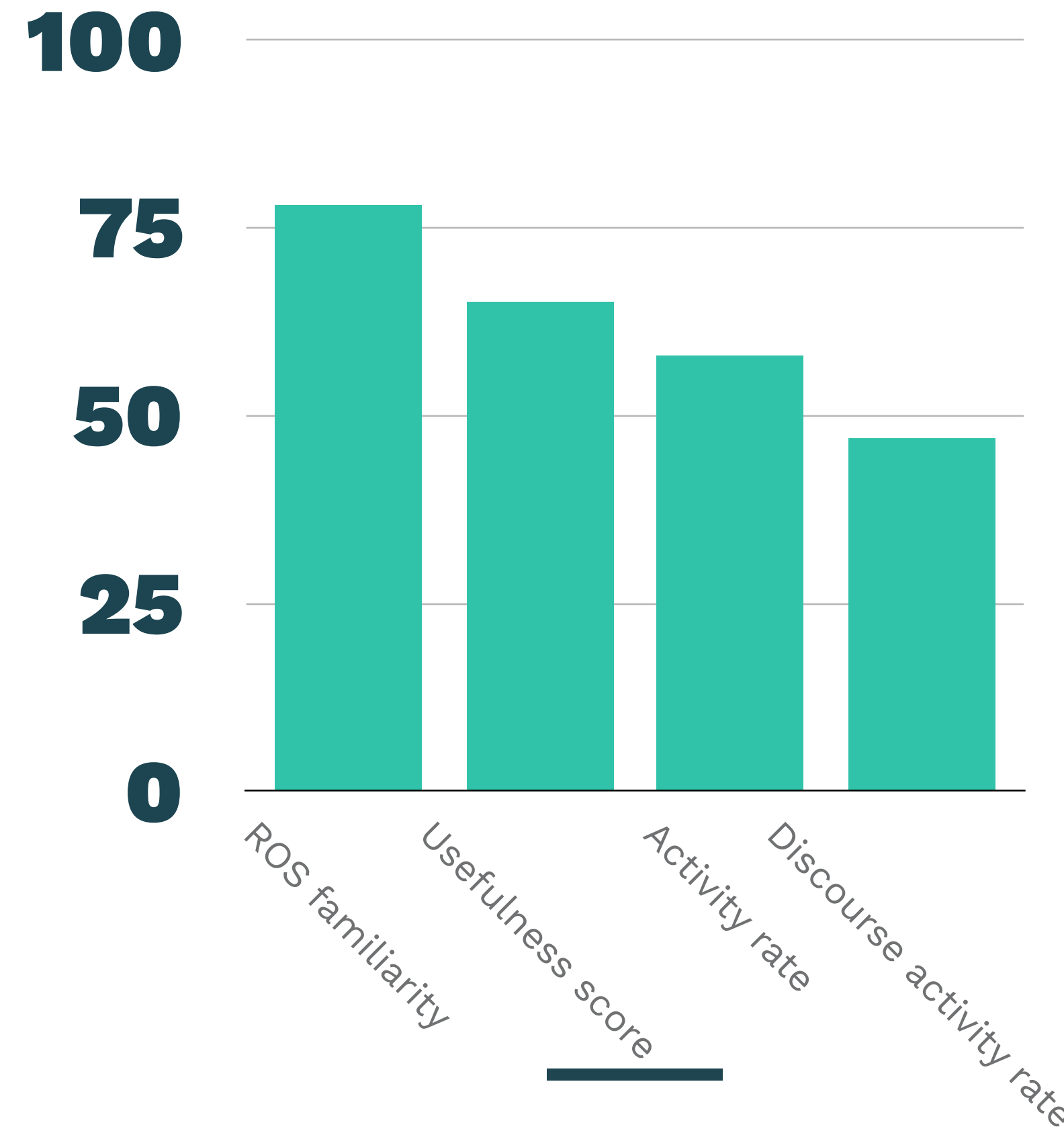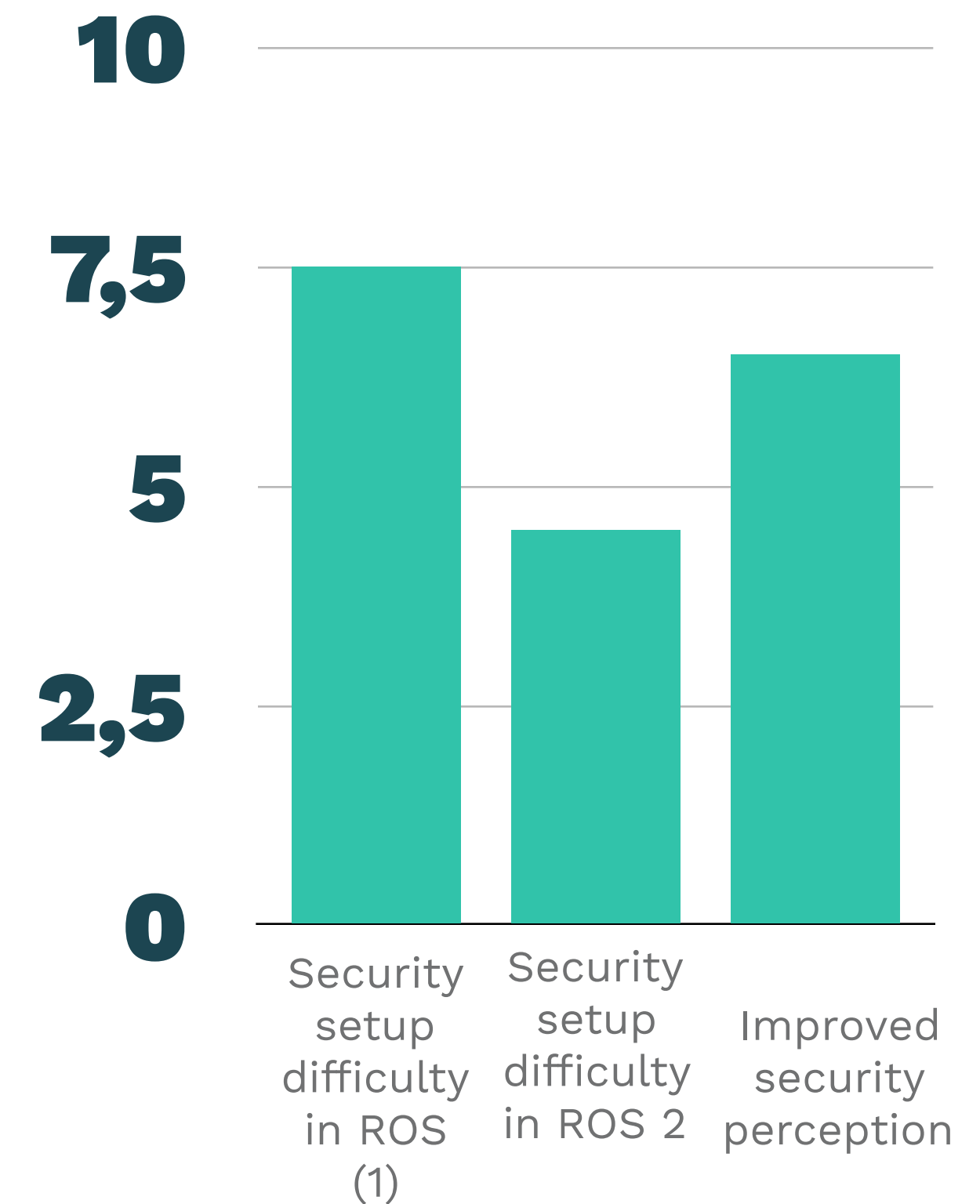
CONFIGURING
SECURITY IN ROS

SECURITY CONSIDERATIONS
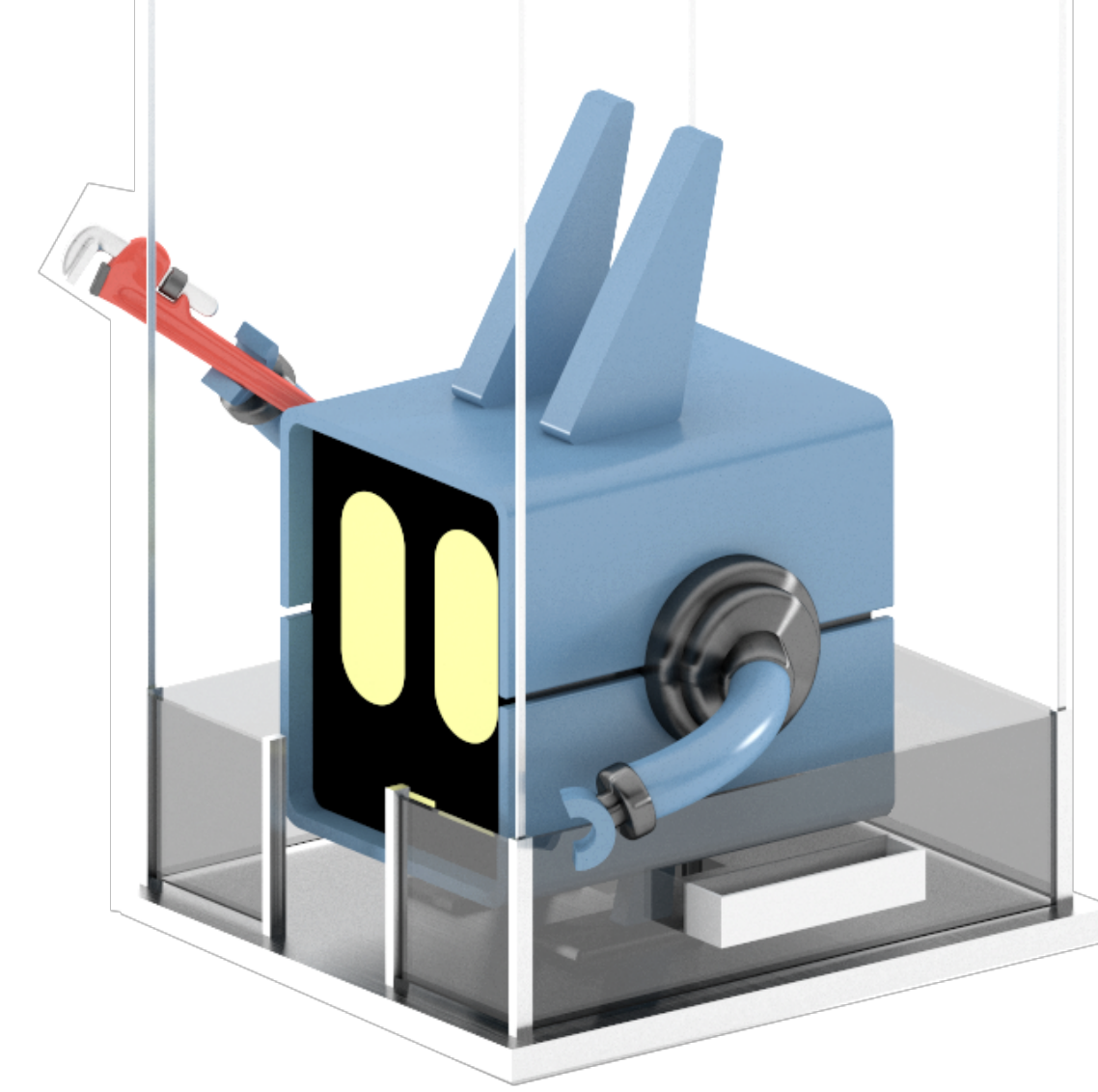
70%

OPEN TO
INVEST

28%

HAVE ACTUALLY
INVESTED
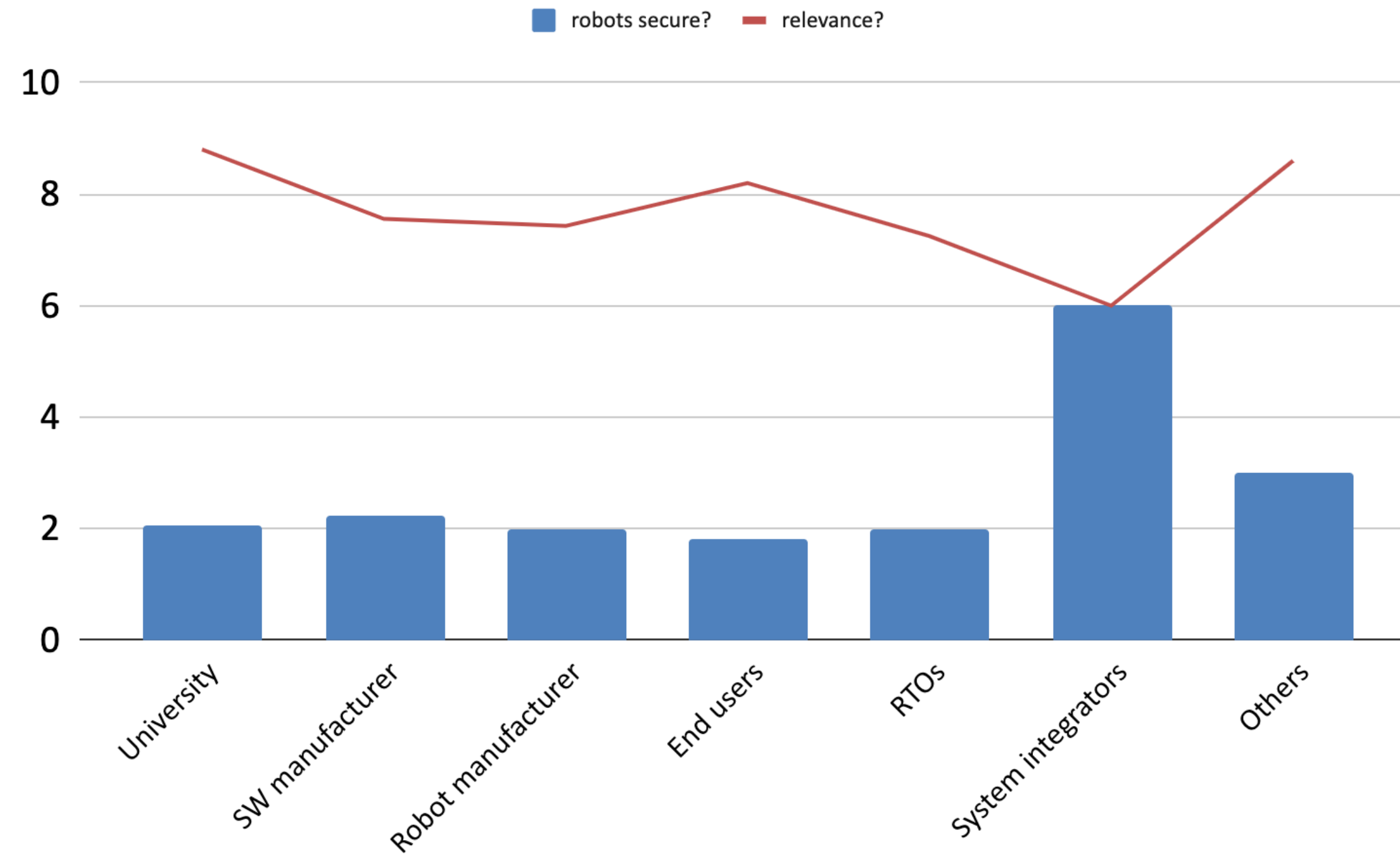
72%

THINK THEY
HAVE NOT
INVESTED
ENOUGH

8.1

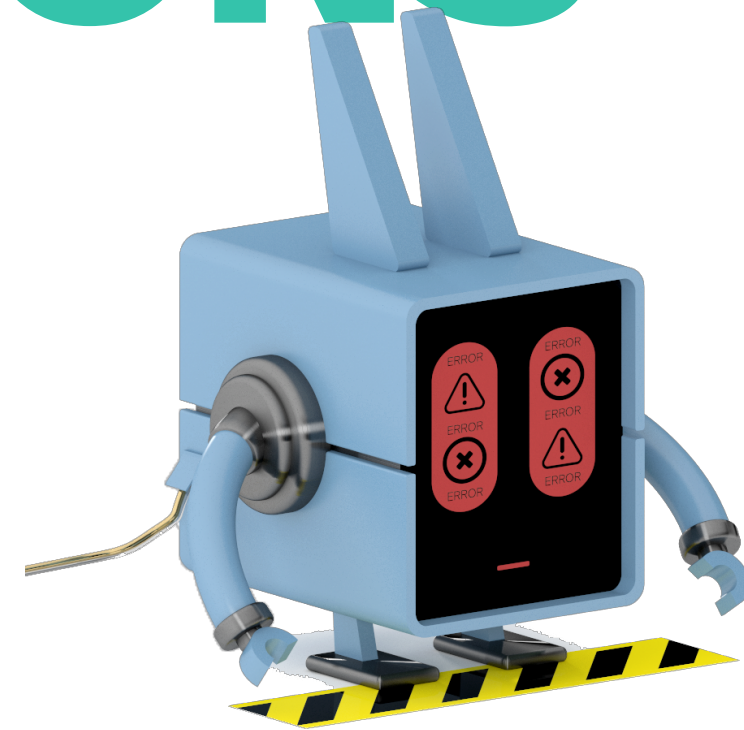SECURITY
RELEVANCE

SECURITY
CONSIDERATIONS

2.4

—

PROTECTED FROM HACKING
AS AN ENDPOINT?

Legend: robots secure? relevance?

PER PLAYER UNSTACKED
RELEVANCE & ENDPOINT SECURITY

(IN)SECURITY OBSERVATIONS

56%

IDENTIFIED
CYBER- WEAKNESSES IN ROBOTS

8%

WITNESSED
A CYBERATTACK

1 EXPOSED
NETWORK SERVICES

2 POTENTIAL
PHYSICAL ATTACKS

3 ISSUES IN
FIRMWARE

3 DANGEROUS
DEFAULTS

SUSPECTED/OBSERVED
VULNERABILITIES

(IN)SECURITY CONCERNS

1	1	1
SAFETY VIOLATIONS	**DATA LOSS**	**BLACKHATS**

2	2	2
DENIAL OF SERVICE	**SAFETY VIOLATIONS**	**UNINTENTIONAL EMPLOYEES**

MOST
LIKELY

MOST
FEARS

BY
COMPLICITS

MITIGATION STRATEGIES

24%
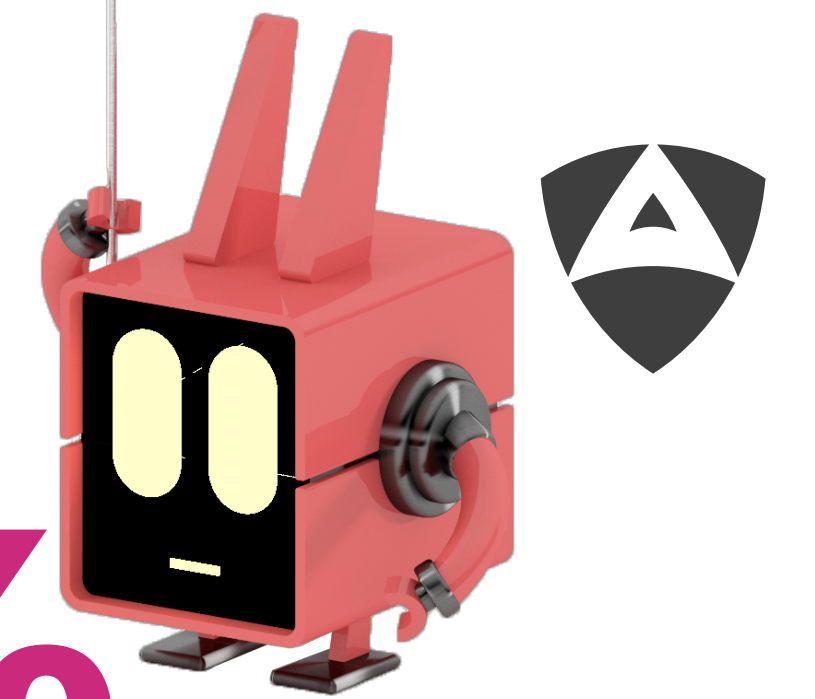
ROBOT SECURITY
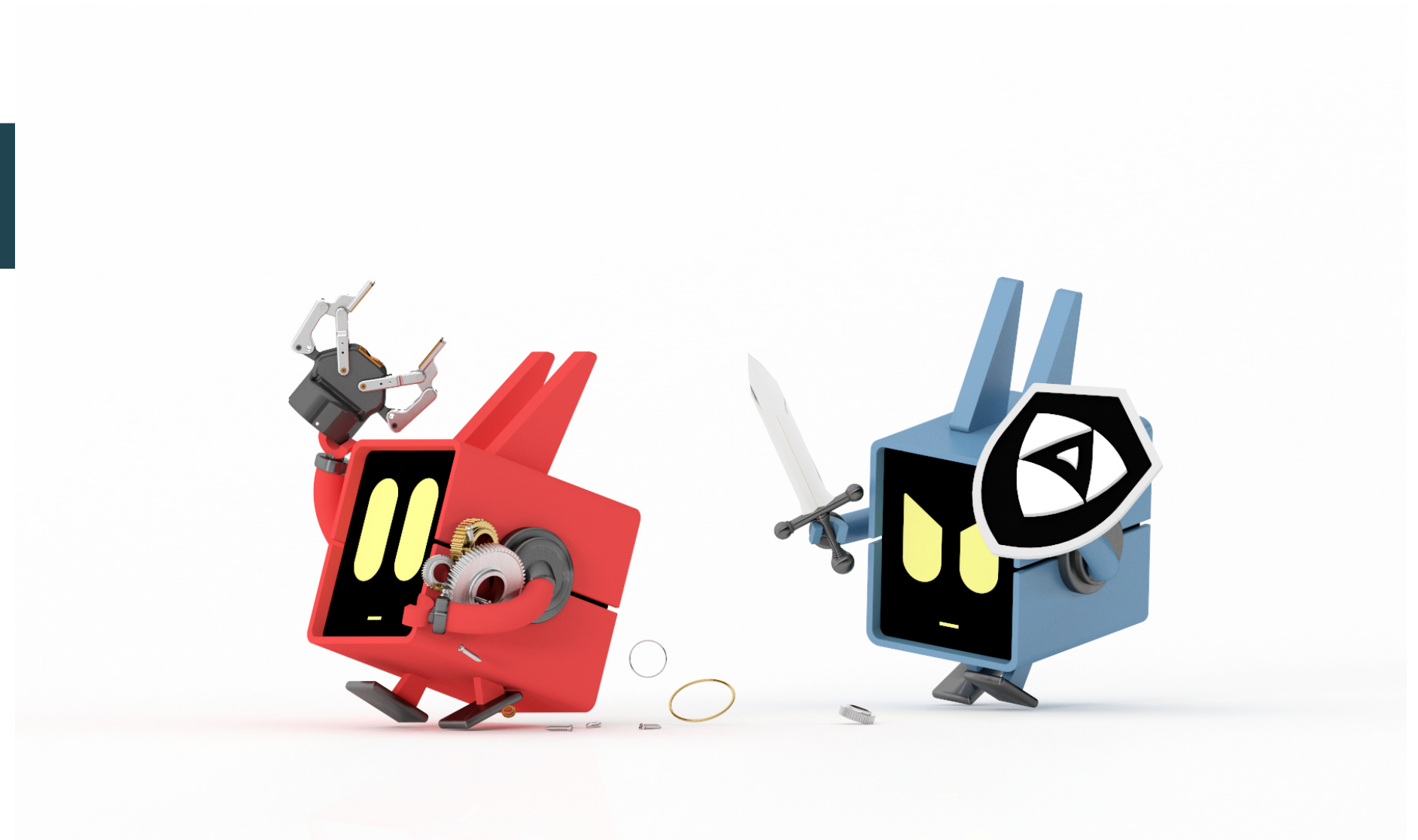**AUDITS**

56%

50%

36%

28%

PERIMETER
FIREWALL, IDS, ETC

NETWORK
SEGMENTATION & MICROSEG

PER ROBOT
MEASURES/ MITIGATIONS

PERFORM
NETWORK SECURITY AUDITS

STANDARDIZATION CONCERNS

42%

AWARENESS IN
SAFETY ASPECTS

22% *

AWARENESS IN
SECURITY STANDARDS

78%

LACK OF
STANDARDS

SOME CONCLUSIONS

- Varied profiles and backgrounds have filled the Robot Security Survey

- Security raise of awareness in roboticist

- Robots in general are perceived as weak endpoints. Few attacks witnessed/declared.

- Not much is done in terms of specific investments. Willingness to do so.

- Unstacked analysis is a very useful tool to understand concerns by actor type. System integrators?

- There is lots to do in terms of robot security standardization
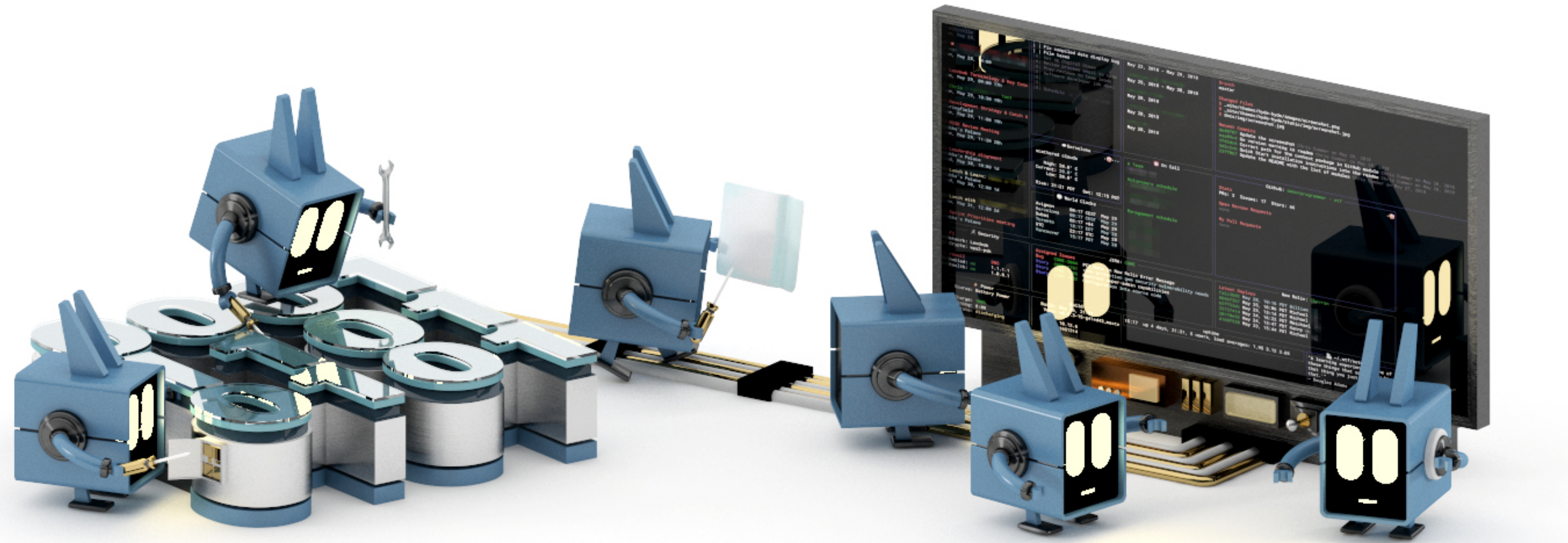
CALL FOR
PARTICIPATION

https://robotsecsurvey.typeform.com/to/u5r44R
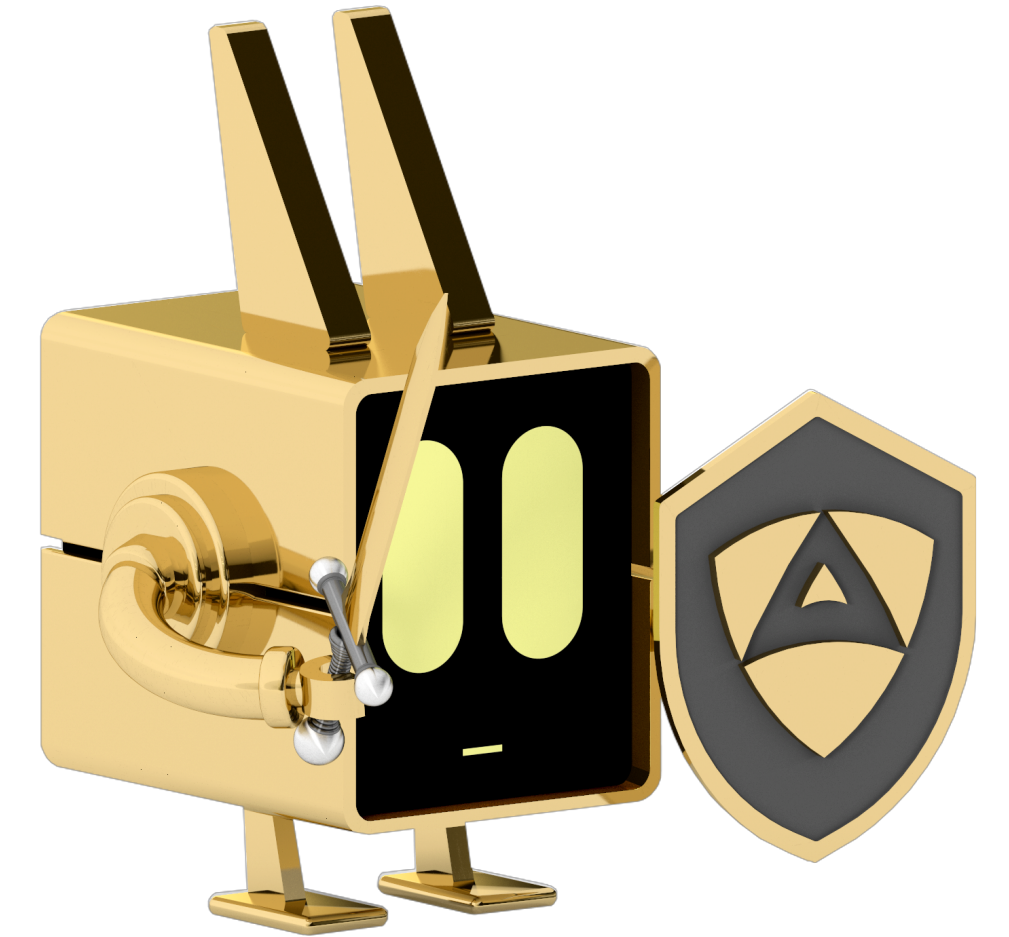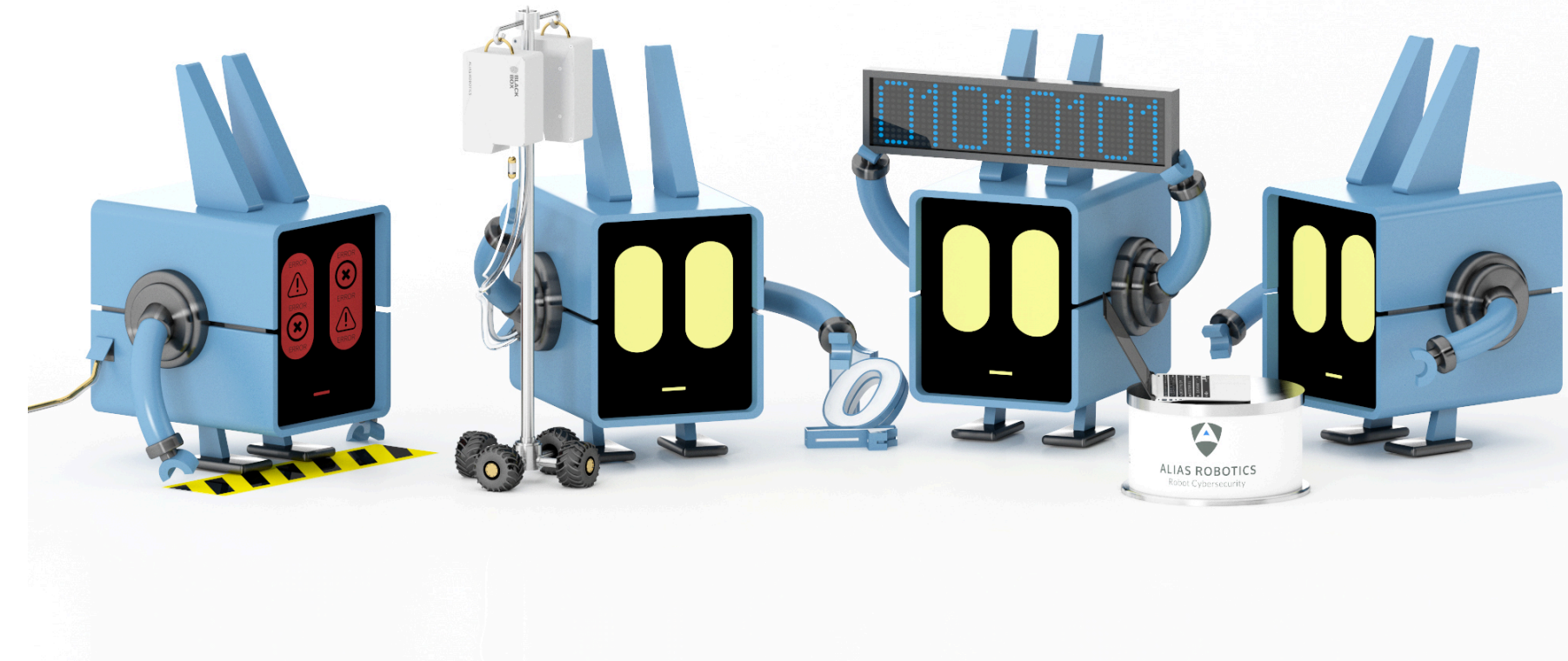
endika@aliasrobotics.com

Robotsecuritysurvey@gmail.com

MILA ESKER!
THANK YOU!

endika@aliasrobotics.com