DEFENSIVE AND OFFENSIVE

ROBOT SECURITY

ALIAS ROBOTICS

Robot Cybersecurity

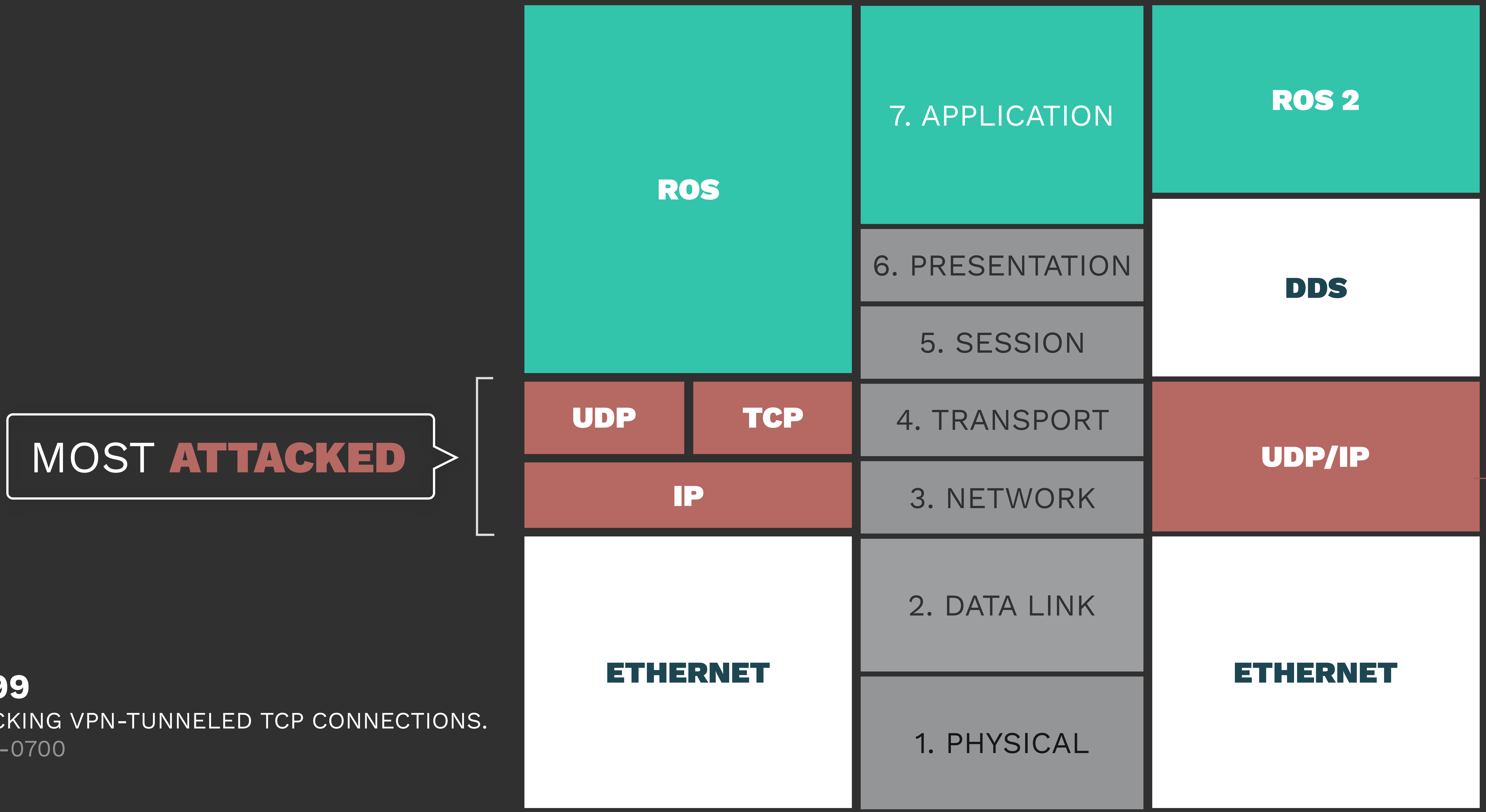
ENDIKA GIL URIARTE

endika@aliasrobotics.com

VÍCTOR MAYORAL VILCHES

victor@aliasrobotics.com

OFFENSIVE
ROBOT SECURITY

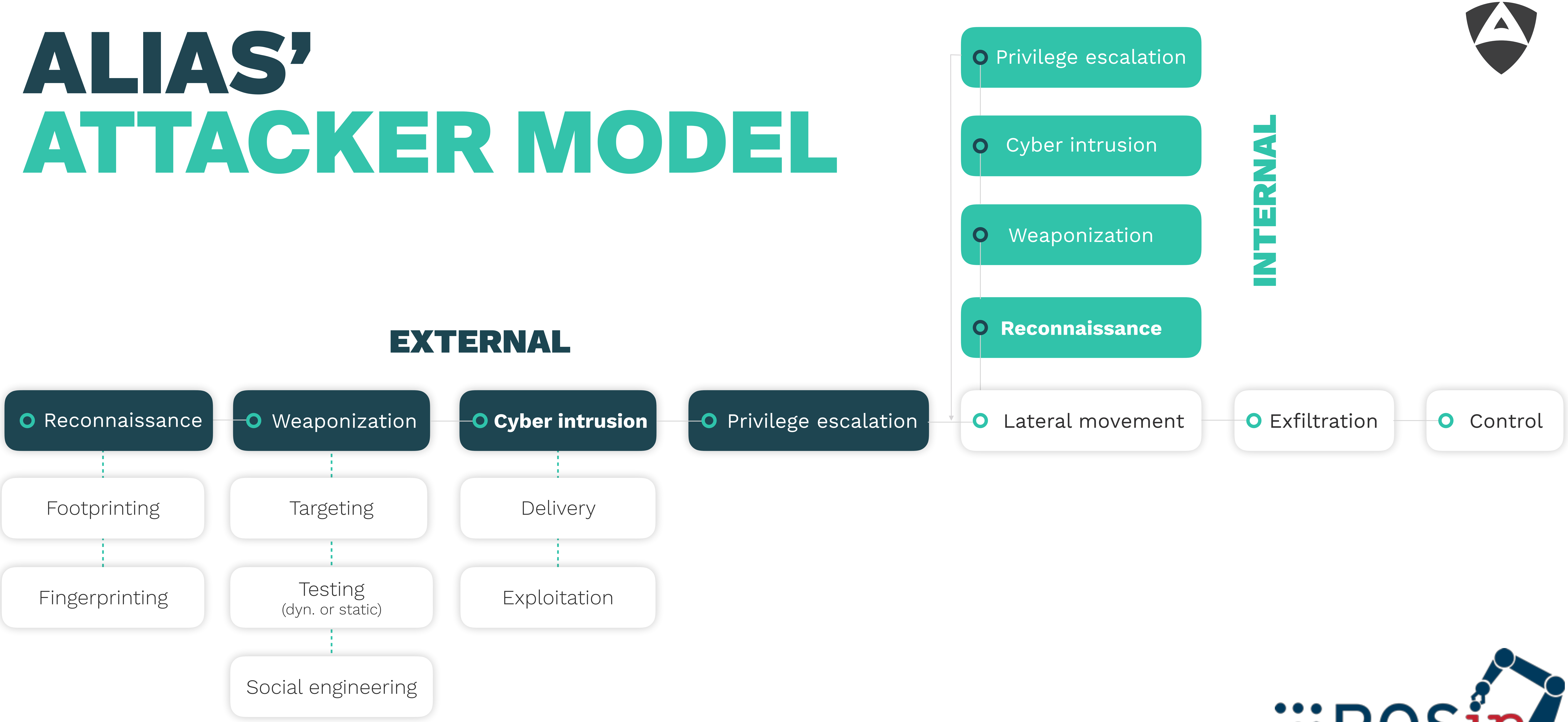


CVE-2019-14899

INFERRING AND HIJACKING VPN-TUNNELED TCP CONNECTIONS.

04 DEC 2019 19:37:07 -0700

ALIAS' ATTACKER MODEL



EXTERNAL

Reconnaissance → Weaponization → **Cyber intrusion** → Privilege escalation → Lateral movement → Exfiltration → Control

Reconnaissance: Footprinting, Fingerprinting

Weaponization: Targeting, Testing (dyn. or static), Social engineering

Cyber intrusion: Delivery, Exploitation

INTERNAL

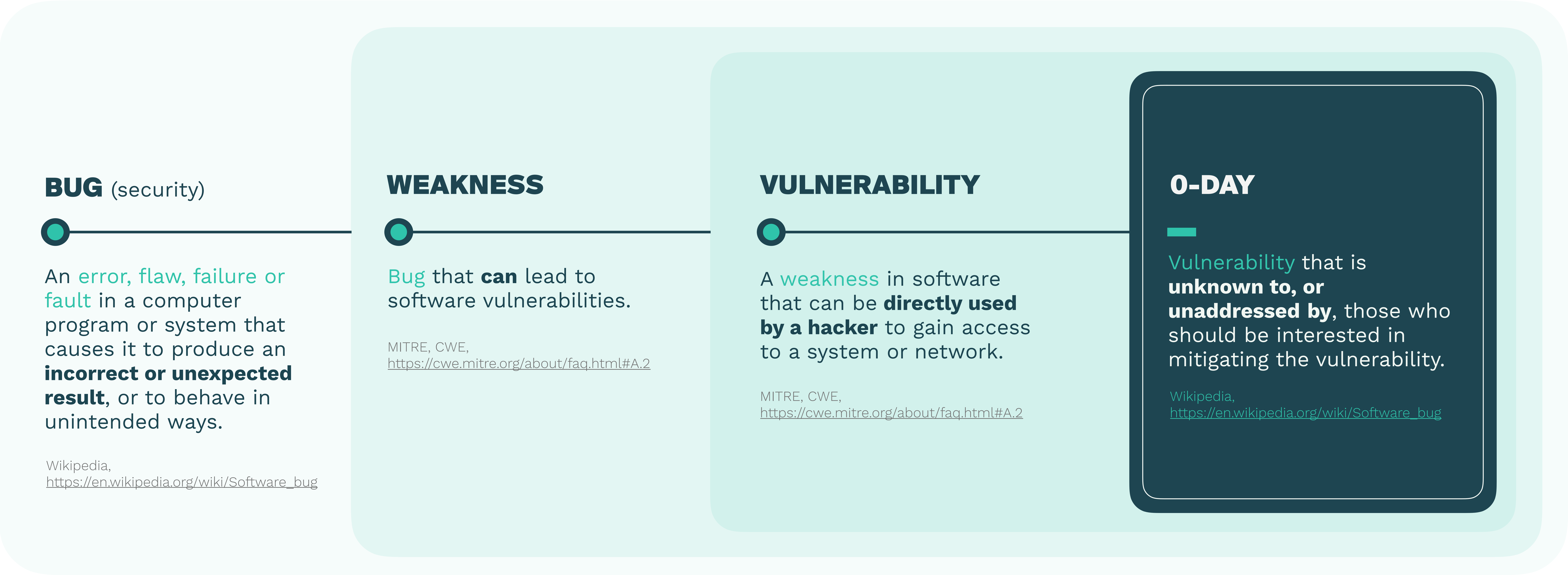
Reconnaissance

Weaponization

Cyber intrusion

Privilege escalation

DEFINING FLAWS



BUG (security)

An error, flaw, failure or fault in a computer program or system that causes it to produce an **incorrect or unexpected result**, or to behave in unintended ways.

Wikipedia,
https://en.wikipedia.org/wiki/Software_bug

WEAKNESS

Bug that **can** lead to software vulnerabilities.

MITRE, CWE,
https://cwe.mitre.org/about/faq.html#A.2

VULNERABILITY

A weakness in software that can be **directly used by a hacker** to gain access to a system or network.

MITRE, CWE,
https://cwe.mitre.org/about/faq.html#A.2

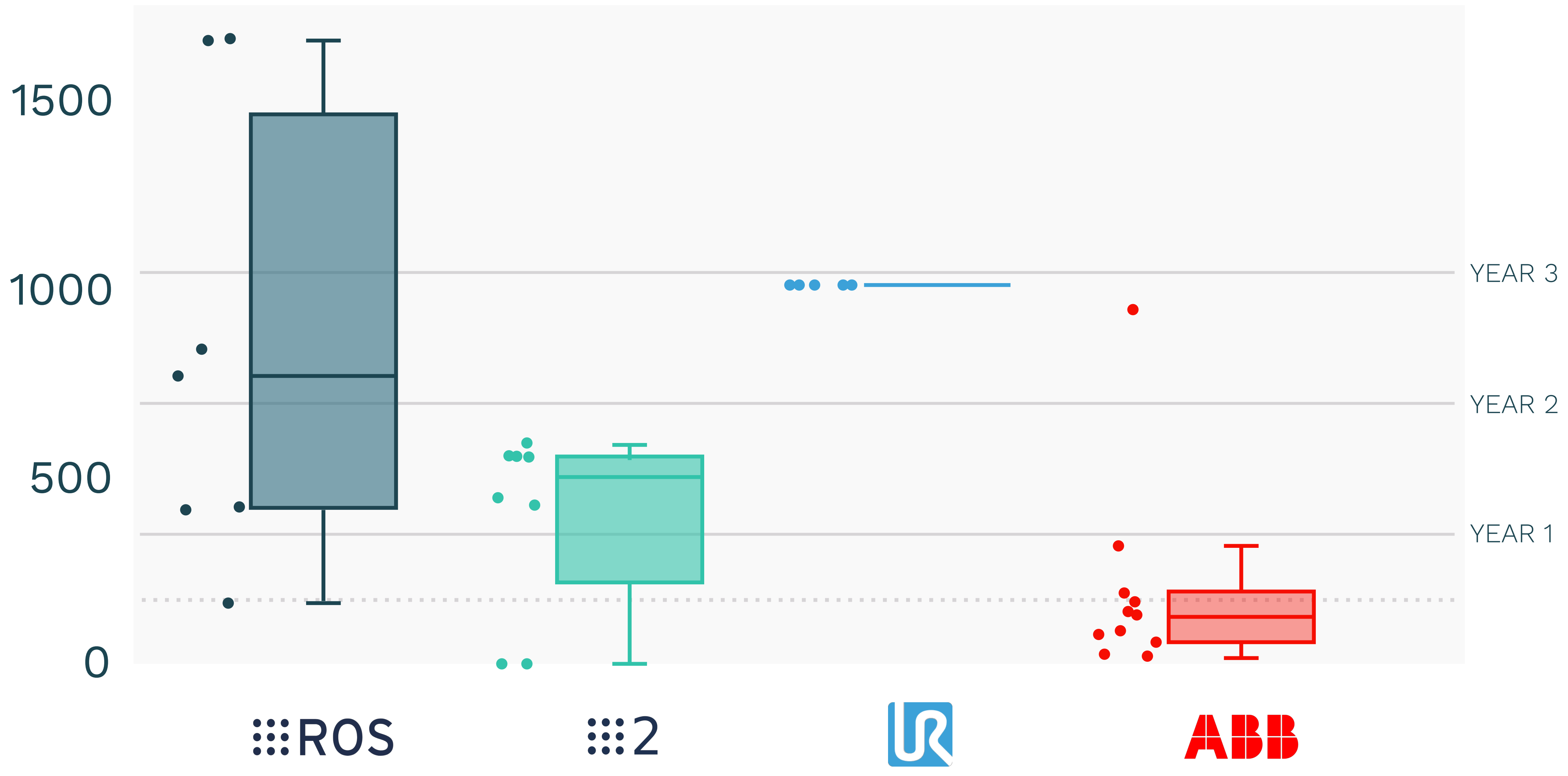
0-DAY

Vulnerability that is **unknown to, or unaddressed by**, those who should be interested in mitigating the vulnerability.

Wikipedia,
https://en.wikipedia.org/wiki/Software_bug

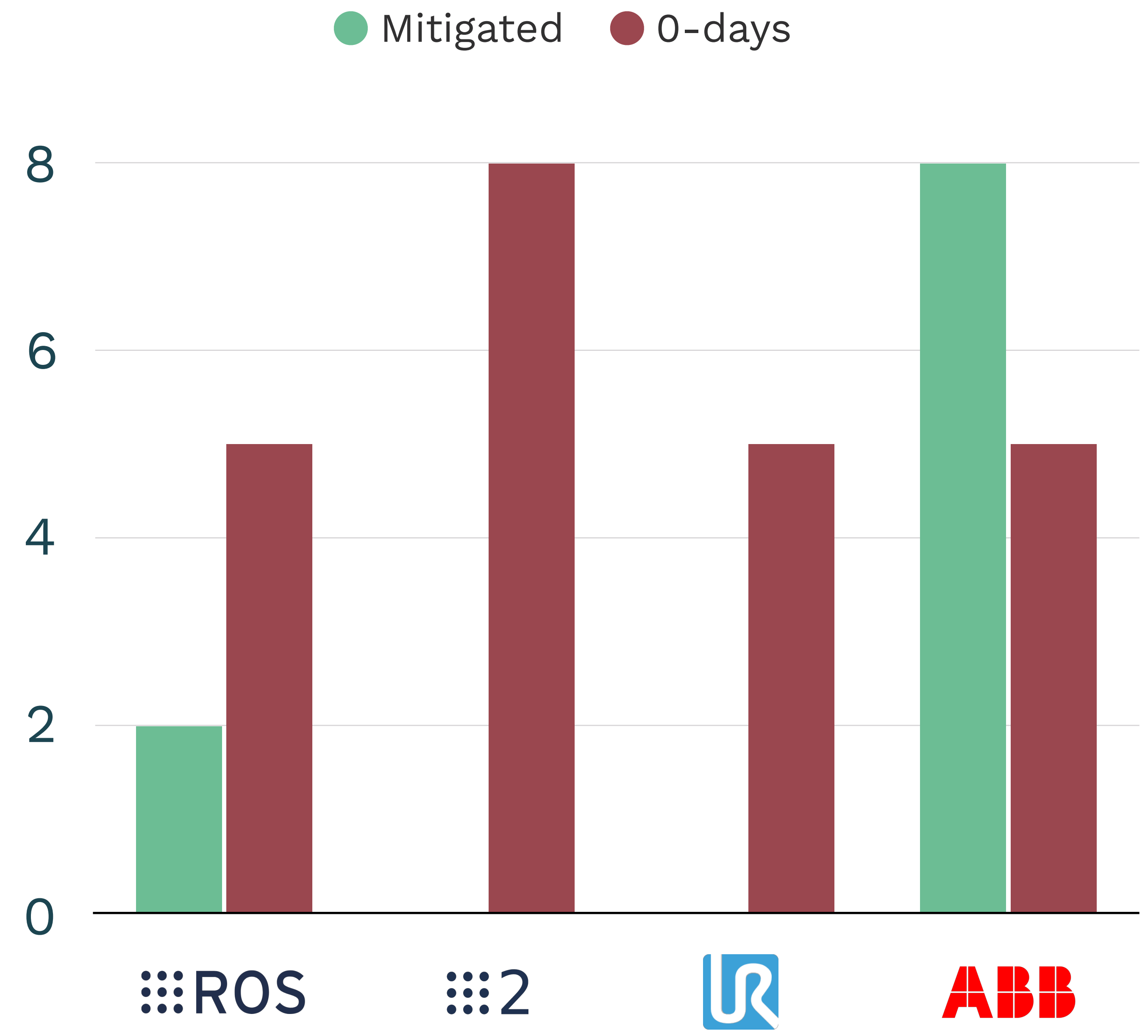
VULNERABILITY MITIGATION AND 0-DAYS

DAYS UNTIL MITIGATION
OR UNTIL TODAY



Data from Robot Vulnerability Database (RVD),
https://github.com/aliasrobotics/RVD,
removed tickets in triage for ROS, ROS2 and UR

0-DAYS
PROPORTION



Data from Robot Vulnerability Database (RVD),
https://github.com/aliasrobotics/RVD,
removed tickets in triage for ROS, ROS2 and UR

VULNERABILITY LANDSCAPE

ROBOT VULNERABILITY DATABASE
(RVD)

	OPEN	CLOSED	ALL
VULNERABILITIES	Vulnerabilities 102	Vulnerabilities 8	Vulnerabilities 110
BUGS	Bugs 79	Bugs 191	Bugs 270
OTHERS	Others 0	Others 1	Others 1

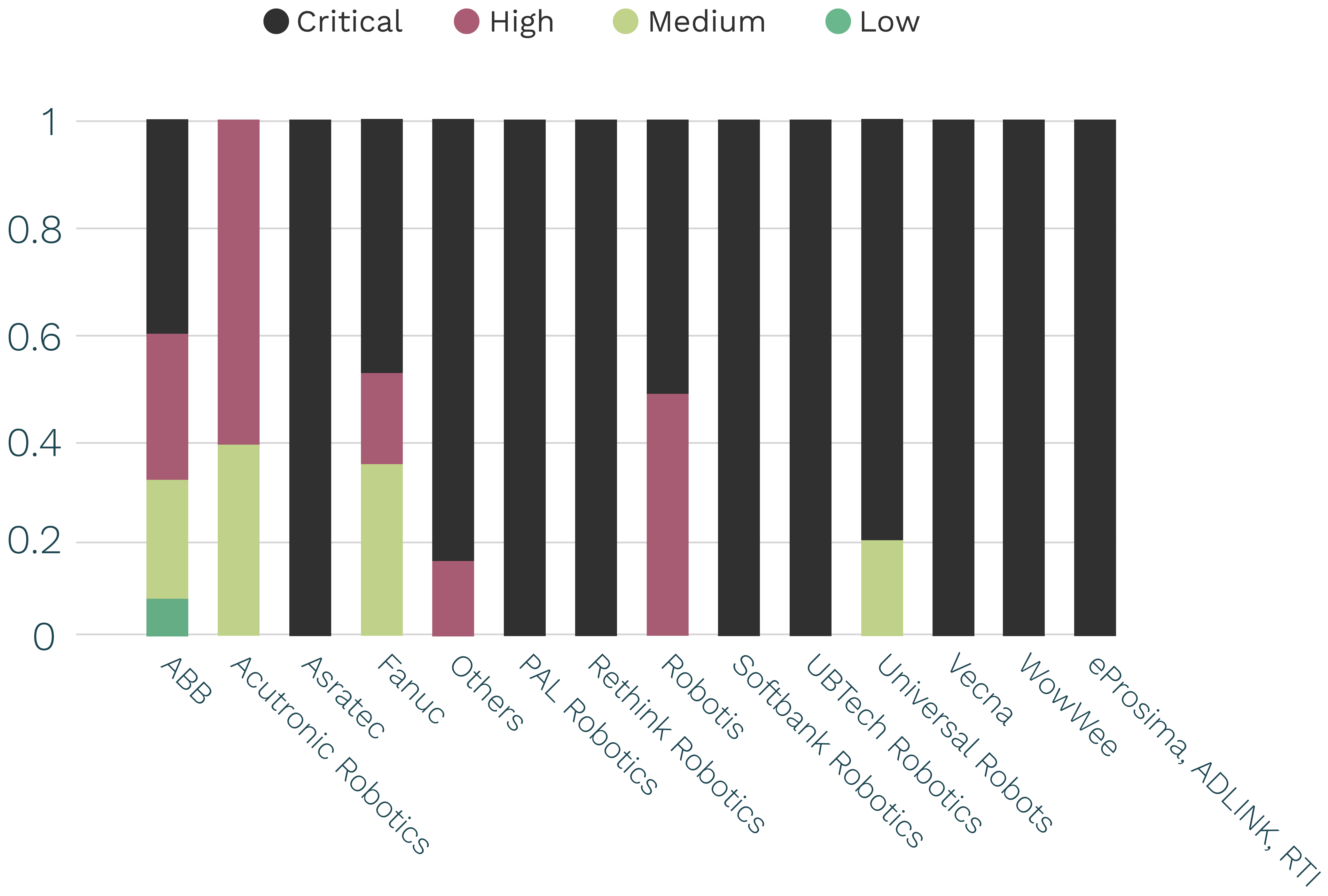
VULNERABILITIES (OPEN)	Vuln.**Critical** 23	Vuln.**High** 23	Vuln.**Medium** 12	Vuln.**Low** 1

Last updated Fri, 06 Dec 2019 23:40:48 GMT

Robot Vulnerability Database (RVD), https://github.com/aliasrobotics/RVD

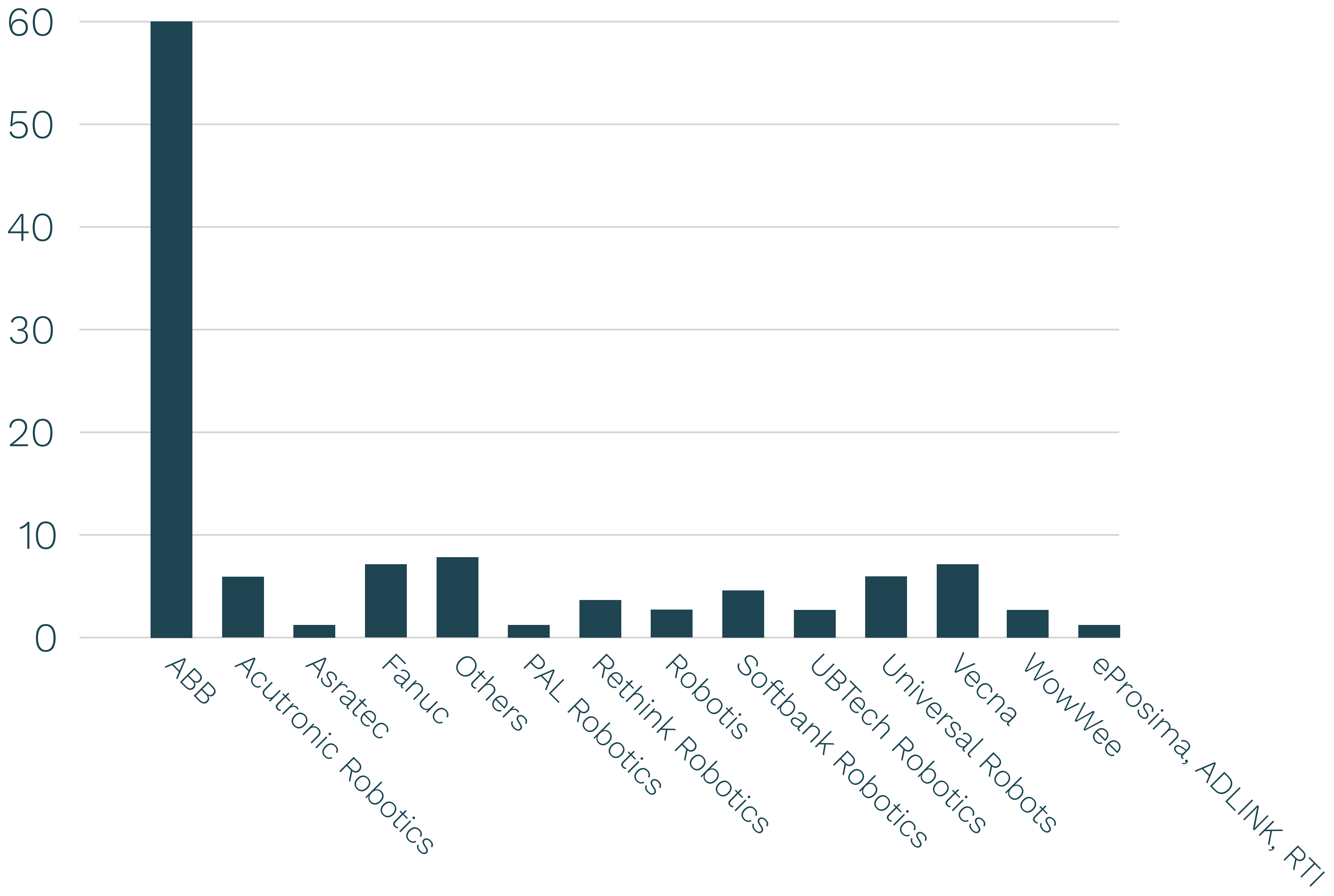
VULNERABILITY LANDSCAPE

SEVERITY IN OPEN TICKETS
BY MANUFACTURER



Data from Robot Vulnerability Database (RVD),
https://github.com/aliasrobotics/RVD,

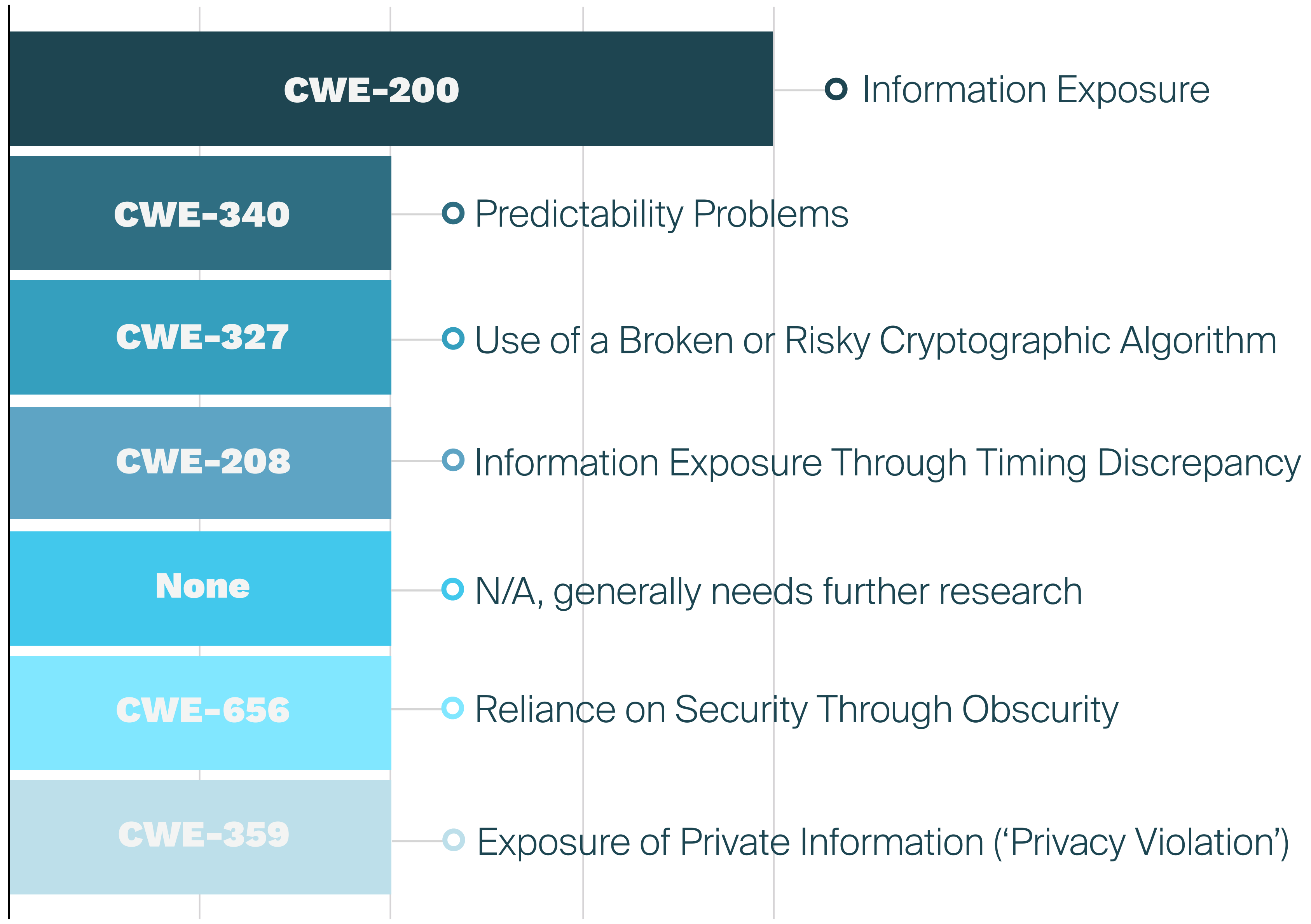
VULNERABILITIES
BY VENDOR (PUBLIC)



Data from Robot Vulnerability Database (RVD),
https://github.com/aliasrobotics/RVD,

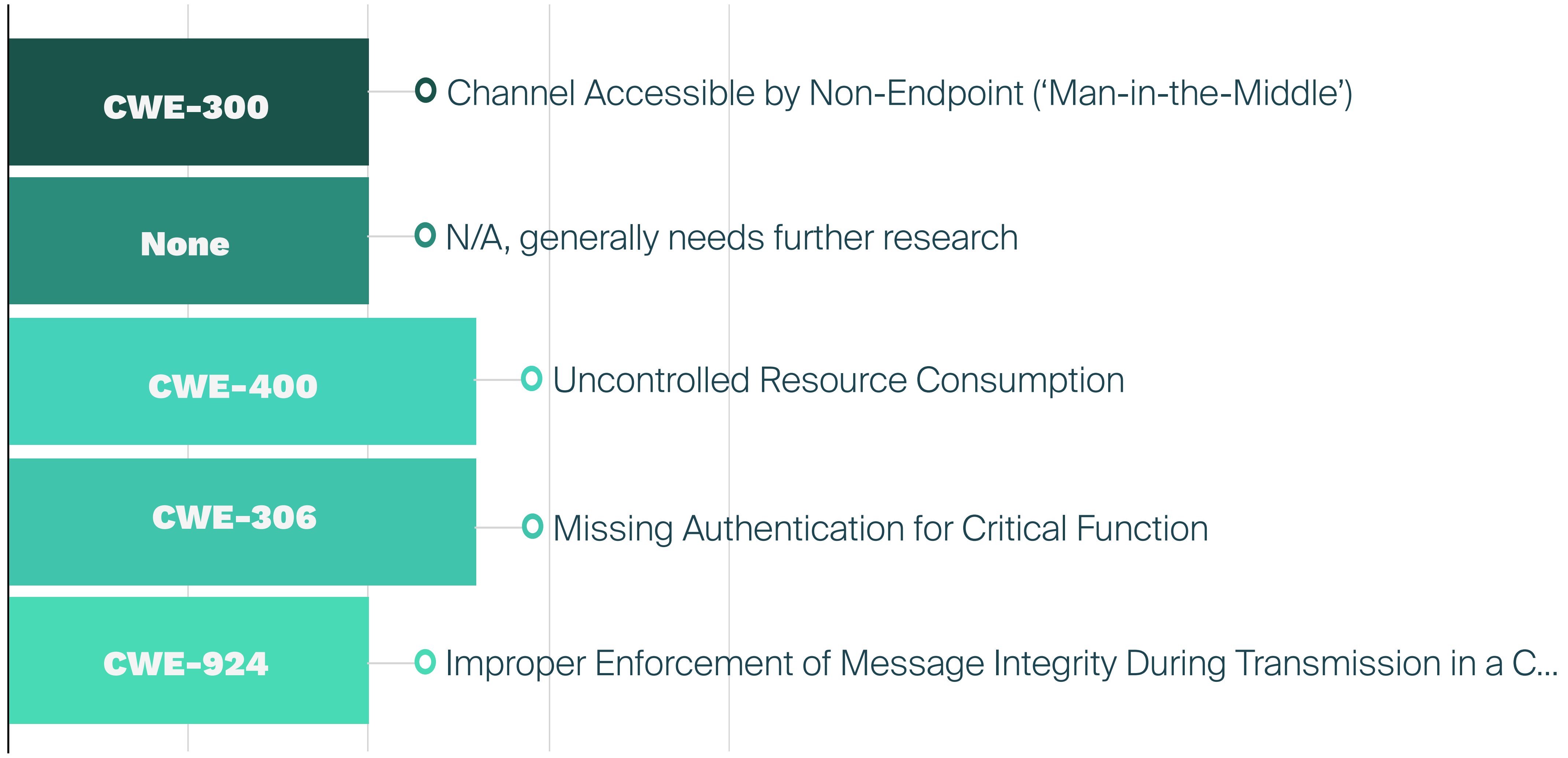
VULNERABILITY LANDSCAPE FOR ROS

VULNERABILITY
LANDSCAPE FOR **ROS**



Data from Robot Vulnerability Database (RVD),
https://github.com/aliasrobotics/RVD,

VULNERABILITY
LANDSCAPE FOR **ROS2**

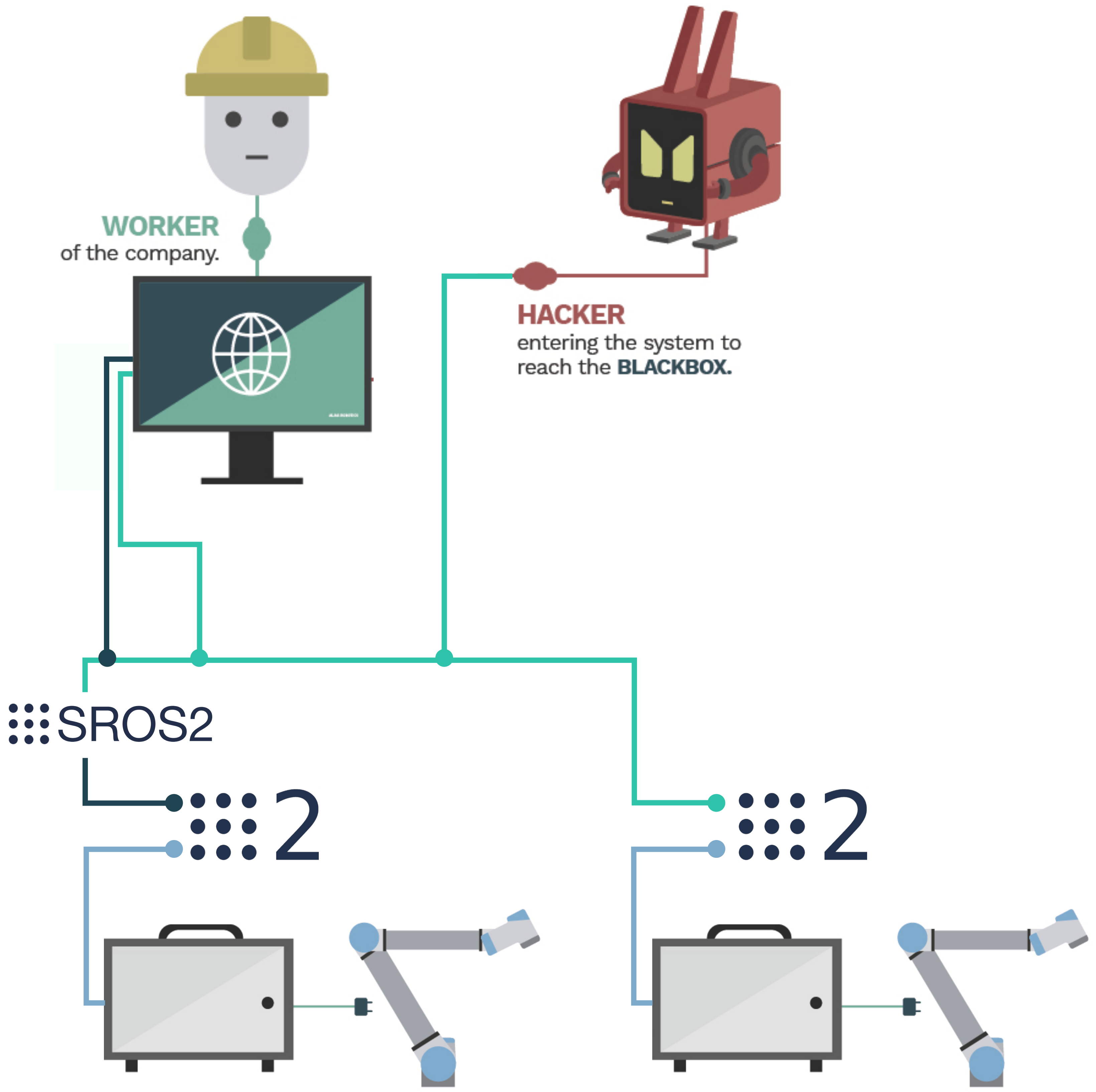


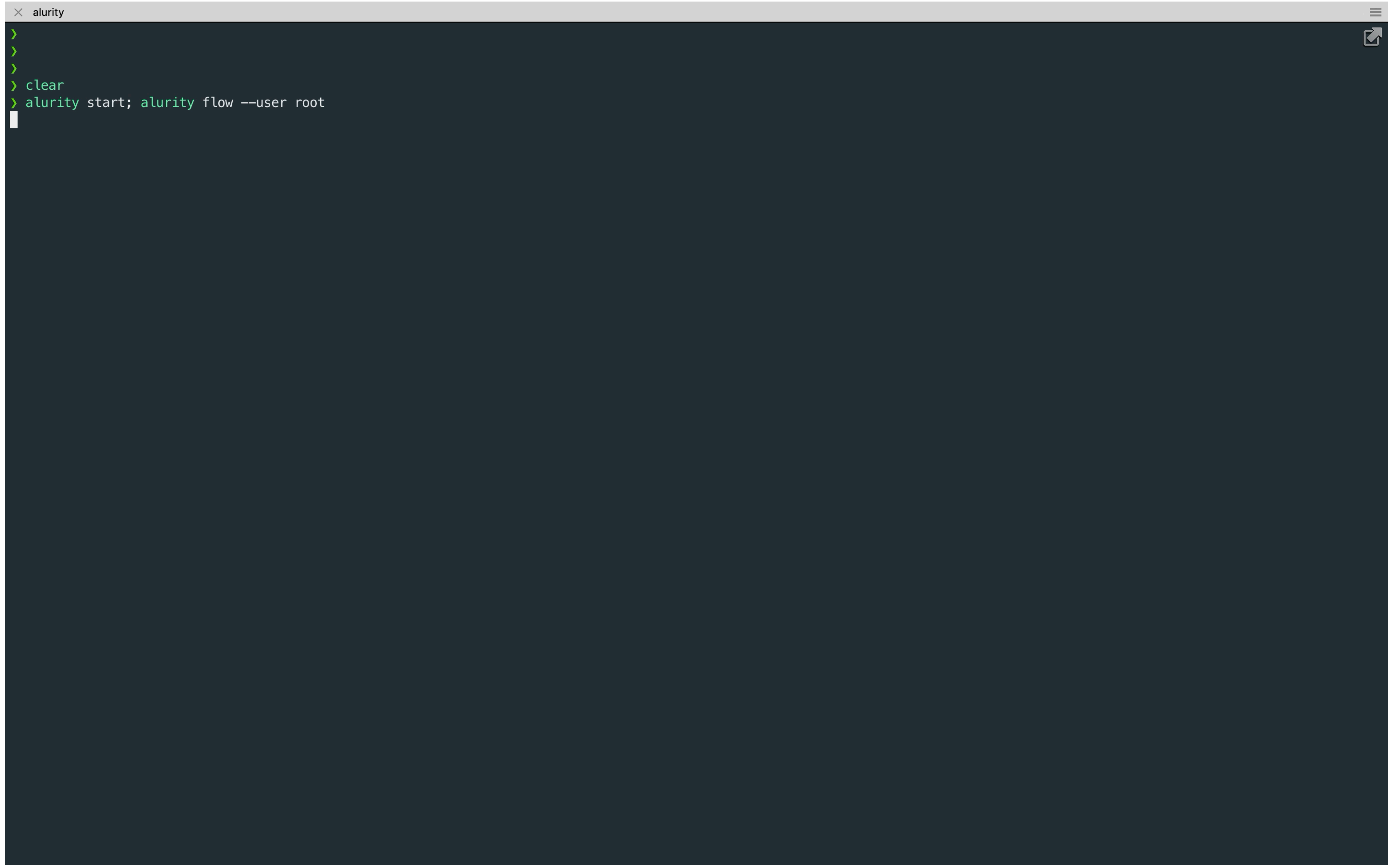
Data from Robot Vulnerability Database (RVD),
https://github.com/aliasrobotics/RVD,

VULNERABILITY EXPLOITATION

CVE-2019-19625 :

SROS2 leaks node information

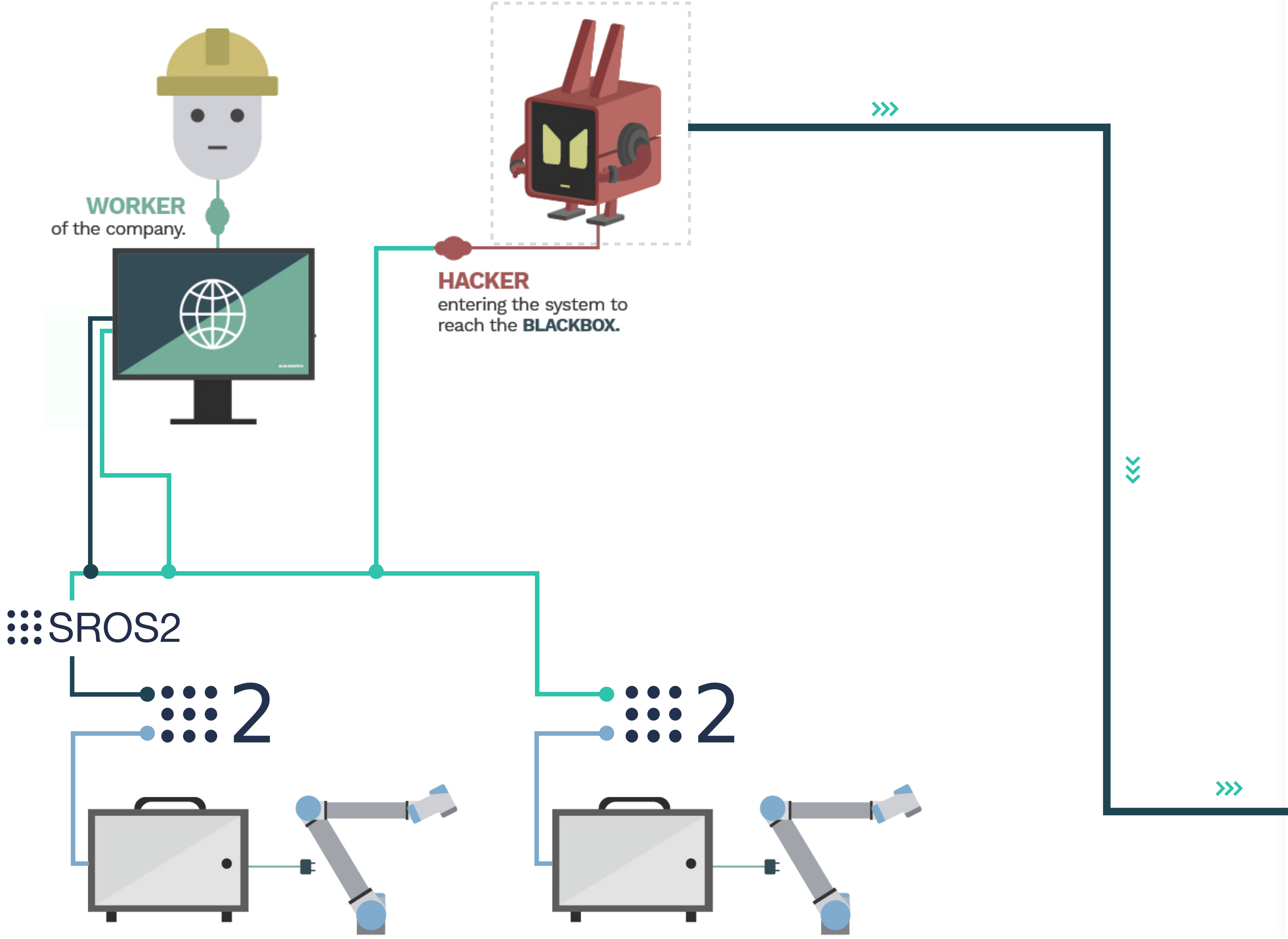


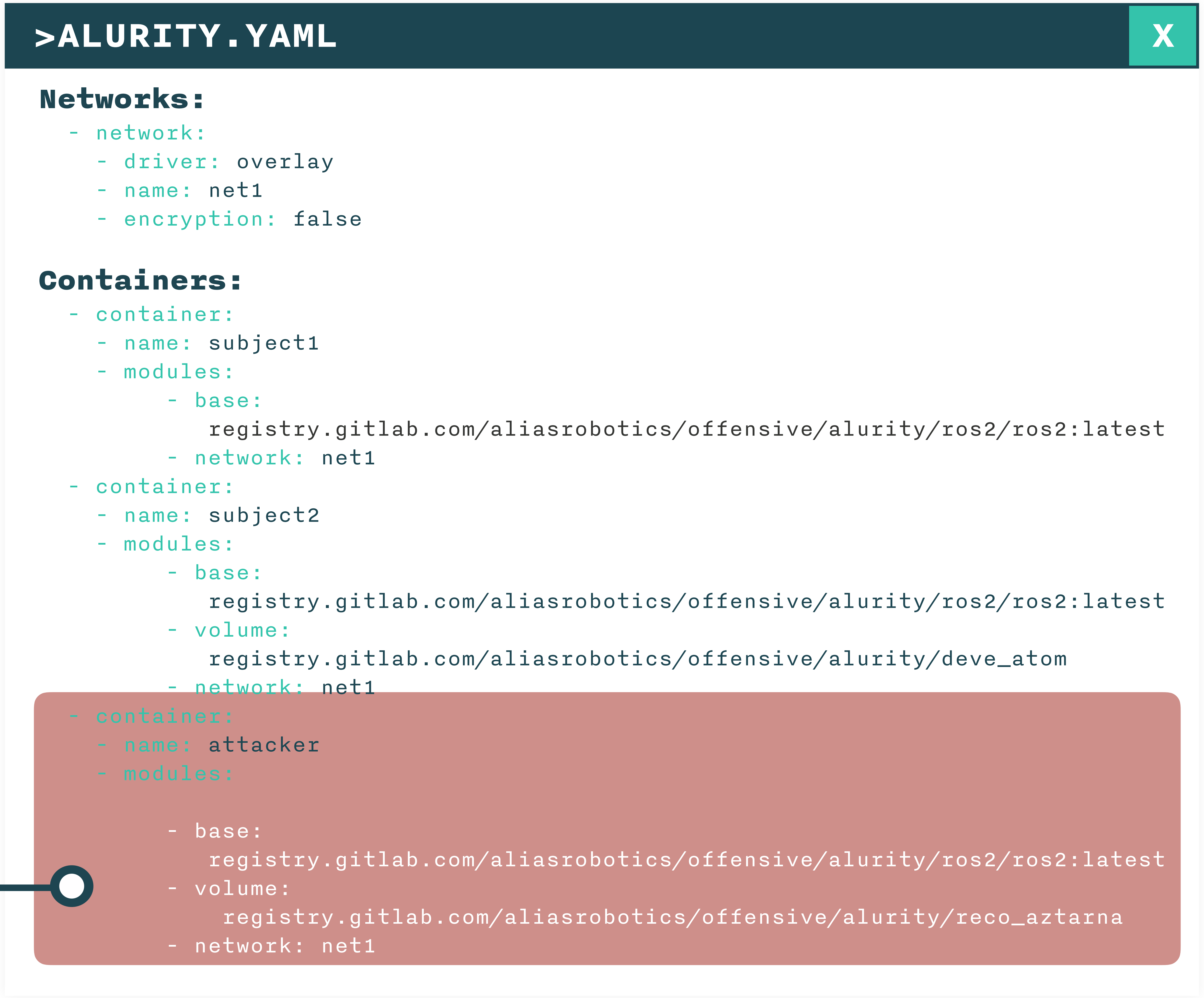


```
❯
❯
❯
❯ clear
❯ alurity start; alurity flow --user root
```

VULNERABILITY
EXPLOITATION

CVE-2019-19625:
SROS2 leaks node information




>ALURITY.YAML

```
Networks:
 - network:
  - driver: overlay
  - name: net1
  - encryption: false

Containers:
 - container:
  - name: subject1
  - modules:
     - base:
      registry.gitlab.com/aliasrobotics/offensive/alurity/ros2/ros2:latest
     - network: net1
 - container:
  - name: subject2
  - modules:
     - base:
      registry.gitlab.com/aliasrobotics/offensive/alurity/ros2/ros2:latest
     - volume:
      registry.gitlab.com/aliasrobotics/offensive/alurity/deve_atom
     - network: net1
 - container:
  - name: attacker
  - modules:

     - base:
      registry.gitlab.com/aliasrobotics/offensive/alurity/ros2/ros2:latest
     - volume:
       registry.gitlab.com/aliasrobotics/offensive/alurity/reco_aztarna
     - network: net1
```

MODULAR AND COMPOSABLE, FOR ROBOTS

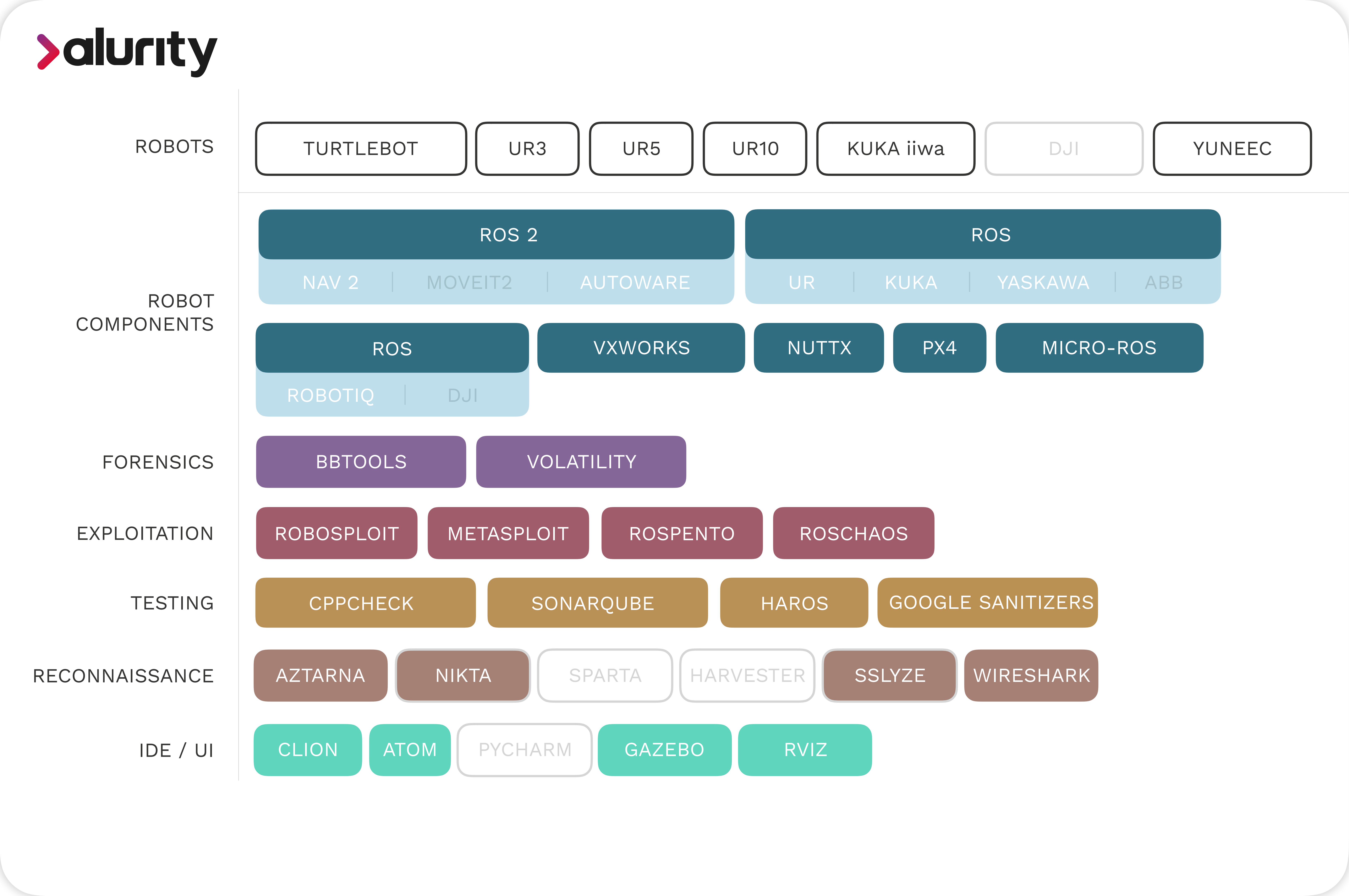
alurity

TOOLBOX FOR ROBOT SECURITY

SOLUTION
ALURITY

TOOLBOX FOR **ROBOT SECURITY**

alurity

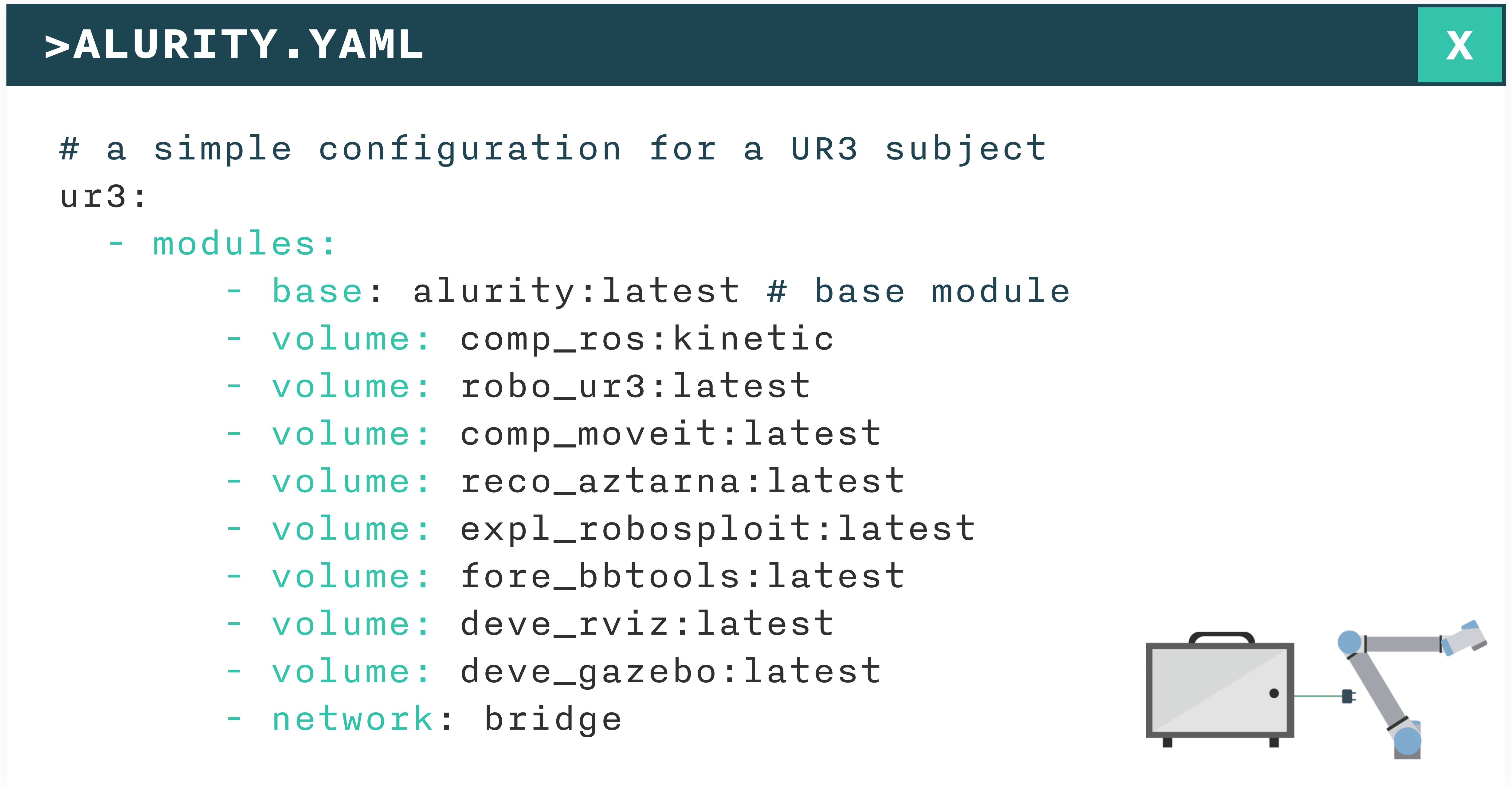


alurity

ROBOTS	TURTLEBOT UR3 UR5 UR10 KUKA iiwa DJI YUNEEC
ROBOT COMPONENTS	ROS 2: NAV 2, MOVEIT2, AUTOWARE ROS: UR, KUKA, YASKAWA, ABB ROS: ROBOTIQ, DJI VXWORKS NUTTX PX4 MICRO-ROS
FORENSICS	BBTOOLS VOLATILITY
EXPLOITATION	ROBOSPLOIT METASPLOIT ROSPENTO ROSCHAOS
TESTING	CPPCHECK SONARQUBE HAROS GOOGLE SANITIZERS
RECONNAISSANCE	AZTARNA NIKTA SPARTA HARVESTER SSLYZE WIRESHARK
IDE / UI	CLION ATOM PYCHARM GAZEBO RVIZ

SOLUTION
ALURITY

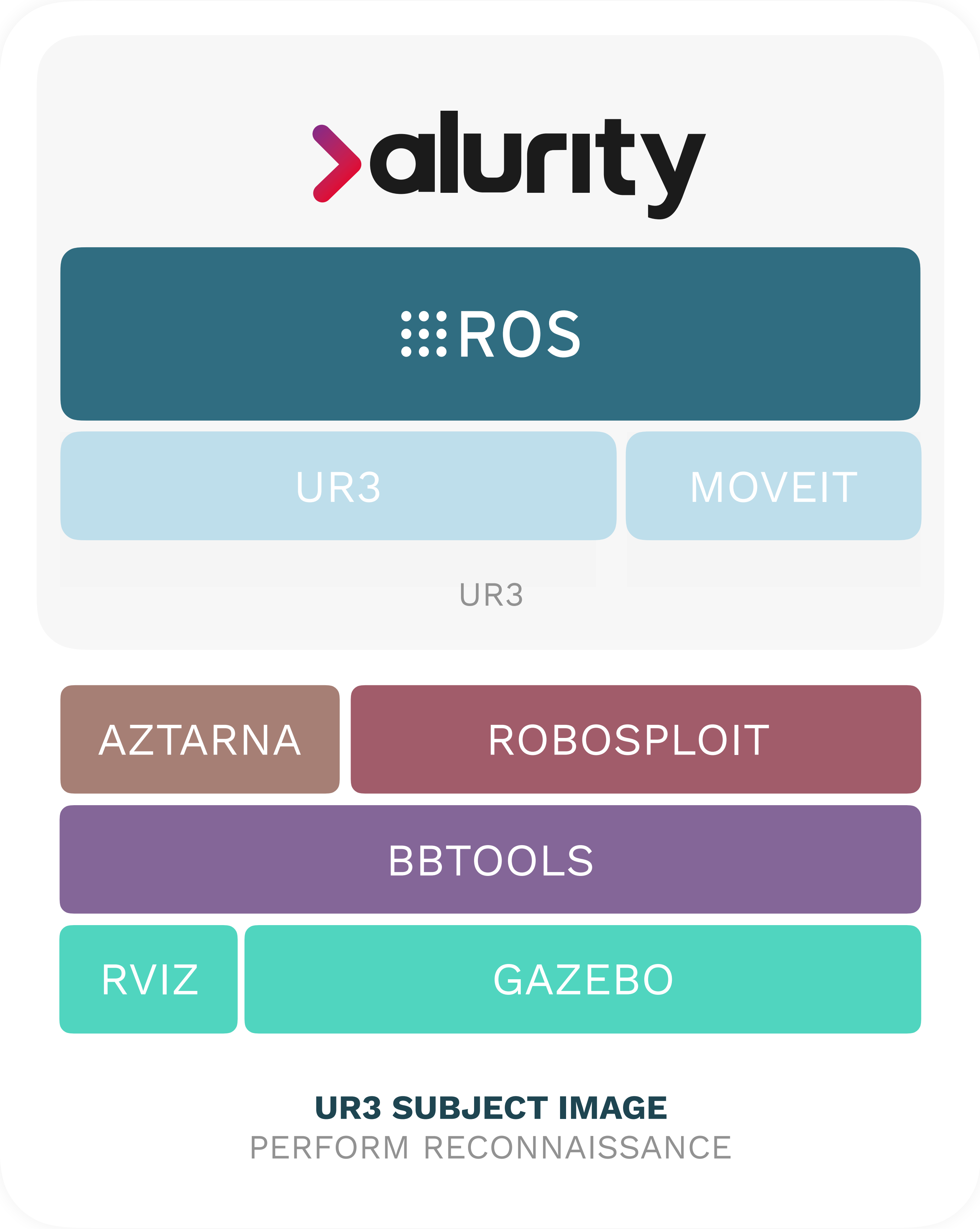
TOOLBOX FOR
ROBOT SECURITY



>ALURITY.YAML

X

```
# a simple configuration for a UR3 subject
ur3:
  - modules:
        - base: alurity:latest # base module
        - volume: comp_ros:kinetic
        - volume: robo_ur3:latest
        - volume: comp_moveit:latest
        - volume: reco_aztarna:latest
        - volume: expl_robosploit:latest
        - volume: fore_bbtools:latest
        - volume: deve_rviz:latest
        - volume: deve_gazebo:latest
        - network: bridge
```



>alurity

ROS

UR3	MOVEIT

UR3

AZTARNA	ROBOSPLOIT

BBTOOLS

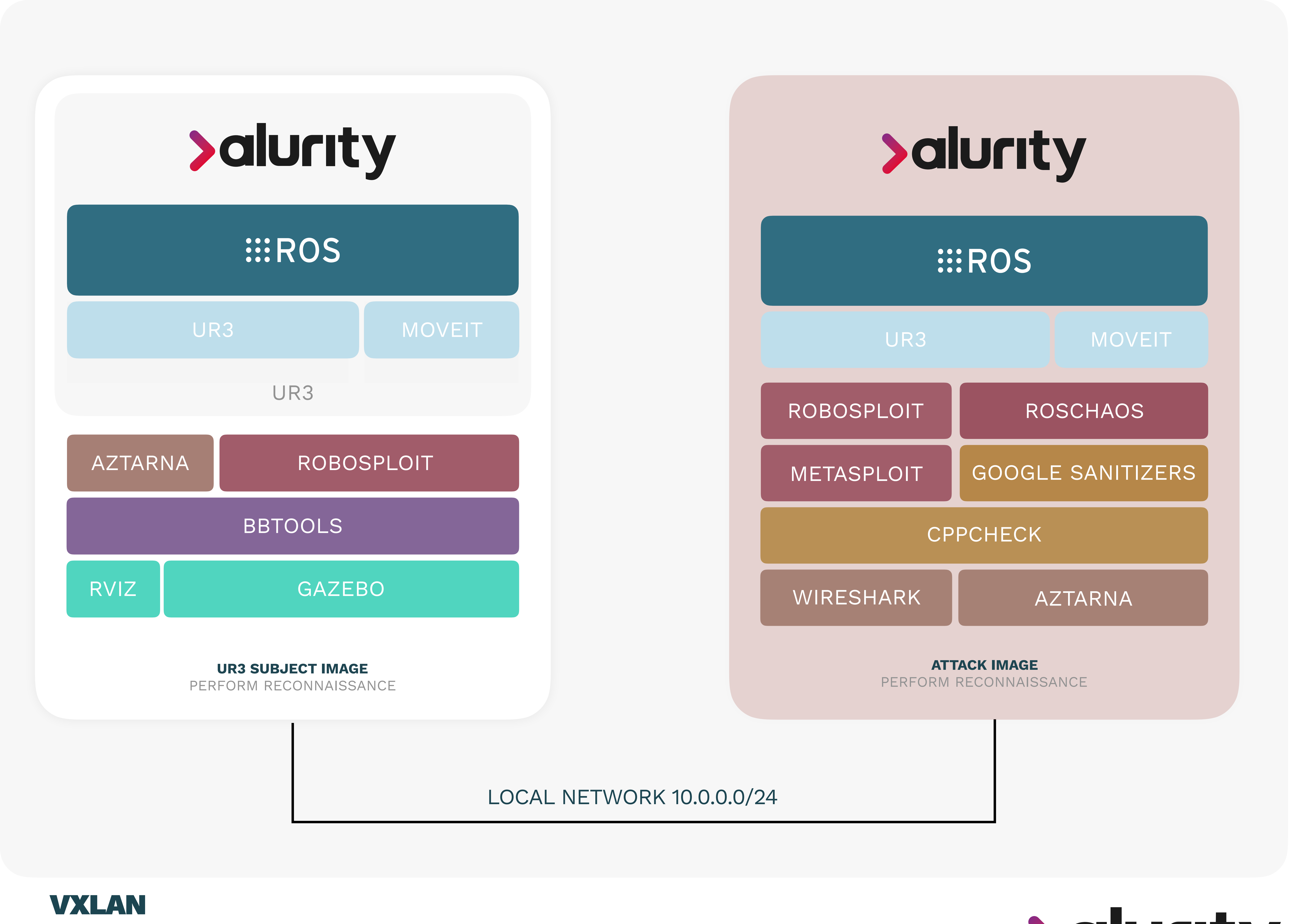
RVIZ	GAZEBO

UR3 SUBJECT IMAGE
PERFORM RECONNAISSANCE

SOLUTION
ALURITY

TOOLBOX FOR **ROBOT SECURITY**

>alurity

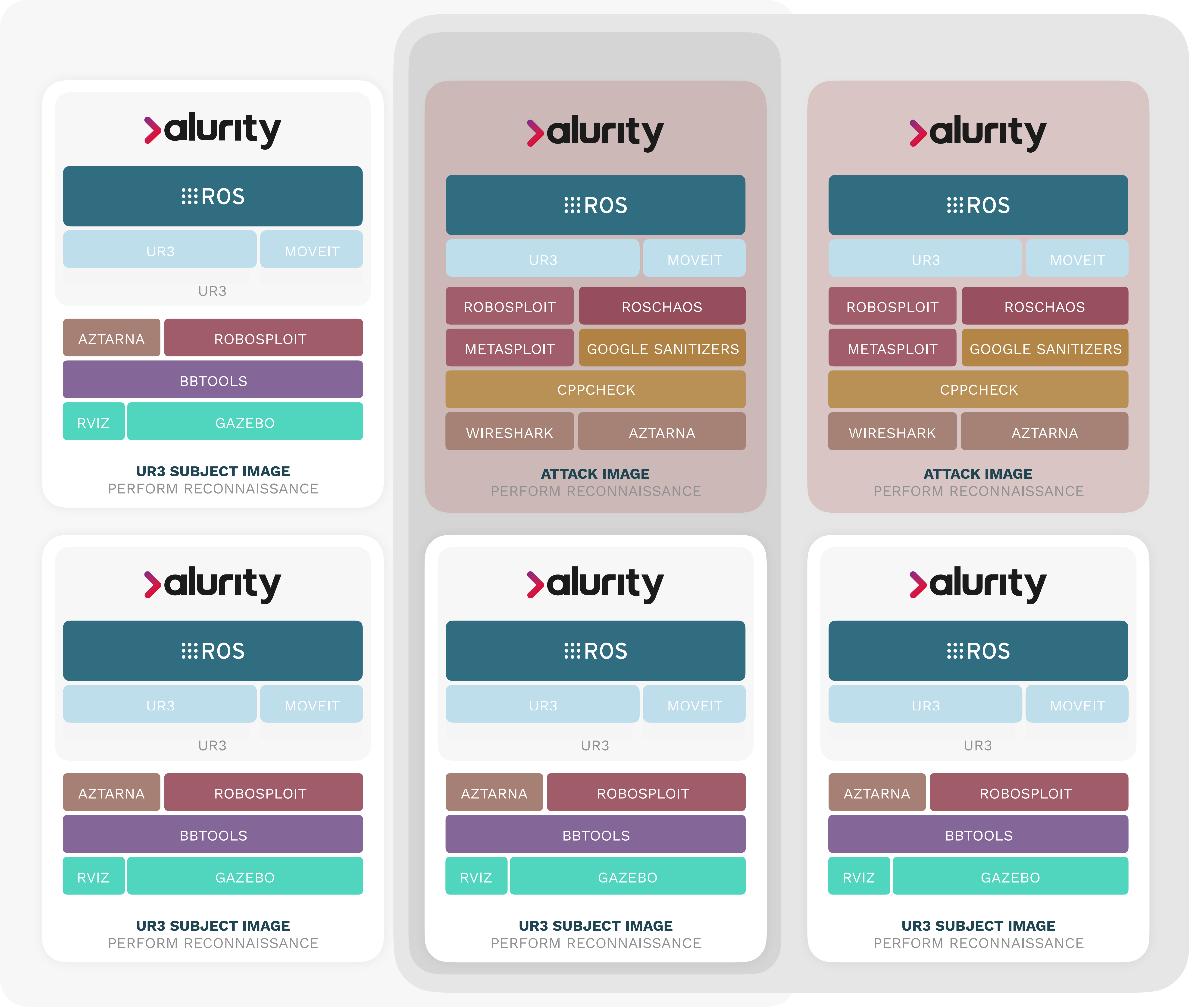


>alurity

SOLUTION ALURITY

TOOLBOX FOR **ROBOT SECURITY**

alurity



alurity

ROS

UR3 | MOVEIT

UR3

AZTARNA | ROBOSPLOIT

BBTOOLS

RVIZ | GAZEBO

UR3 SUBJECT IMAGE
PERFORM RECONNAISSANCE

alurity

ROS

UR3 | MOVEIT

ROBOSPLOIT | ROSCHAOS

METASPLOIT | GOOGLE SANITIZERS

CPPCHECK

WIRESHARK | AZTARNA

ATTACK IMAGE
PERFORM RECONNAISSANCE

alurity

ROS

UR3 | MOVEIT

ROBOSPLOIT | ROSCHAOS

METASPLOIT | GOOGLE SANITIZERS

CPPCHECK

WIRESHARK | AZTARNA

ATTACK IMAGE
PERFORM RECONNAISSANCE

alurity

ROS

UR3 | MOVEIT

UR3

AZTARNA | ROBOSPLOIT

BBTOOLS

RVIZ | GAZEBO

UR3 SUBJECT IMAGE
PERFORM RECONNAISSANCE

alurity

ROS

UR3 | MOVEIT

UR3

AZTARNA | ROBOSPLOIT

BBTOOLS

RVIZ | GAZEBO

UR3 SUBJECT IMAGE
PERFORM RECONNAISSANCE

alurity

ROS

UR3 | MOVEIT

UR3

AZTARNA | ROBOSPLOIT

BBTOOLS

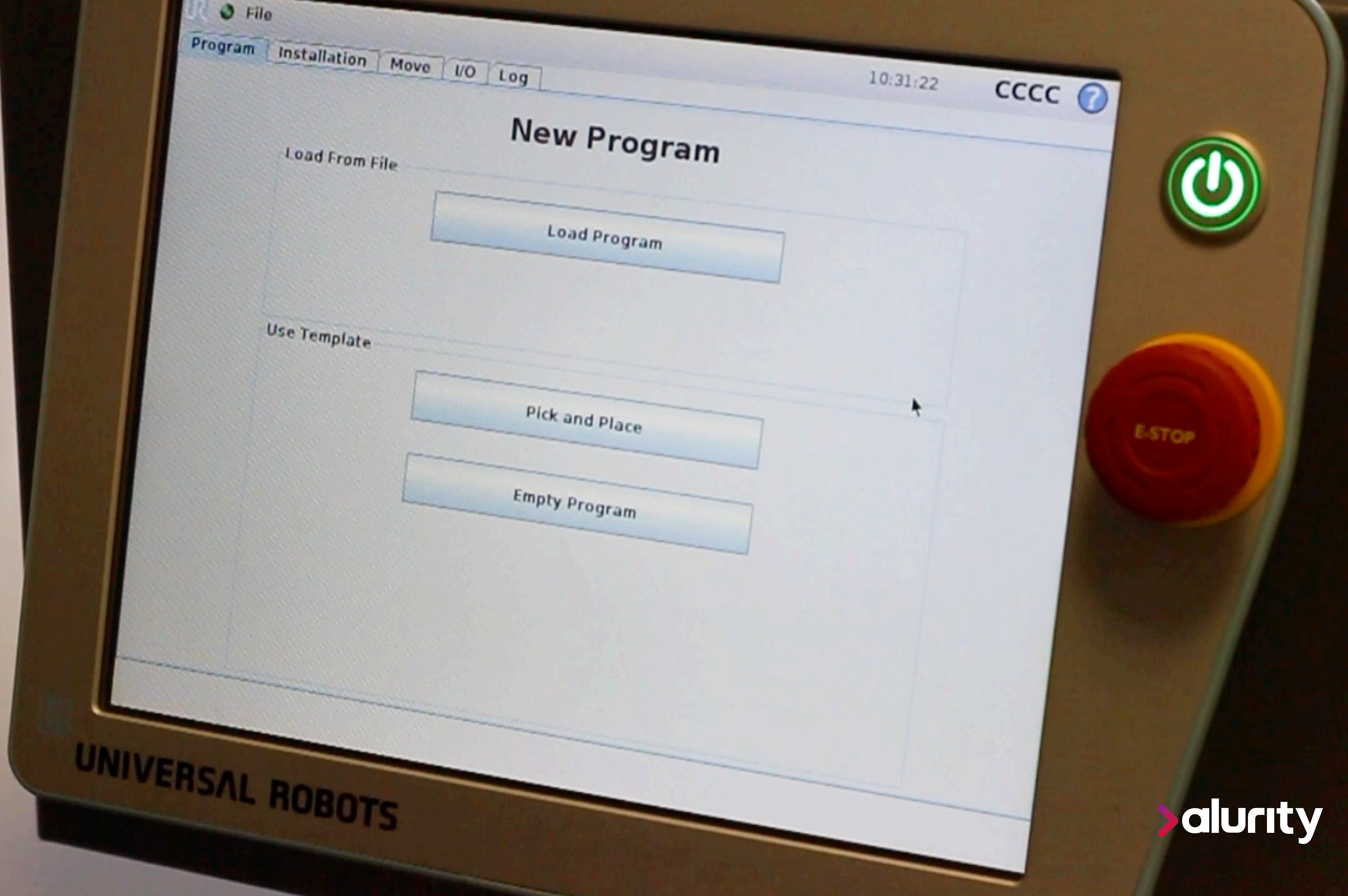
RVIZ | GAZEBO

UR3 SUBJECT IMAGE
PERFORM RECONNAISSANCE

alurity

A STUDY CASE

AKERBELTZ
ROBOT RANSOMWARE

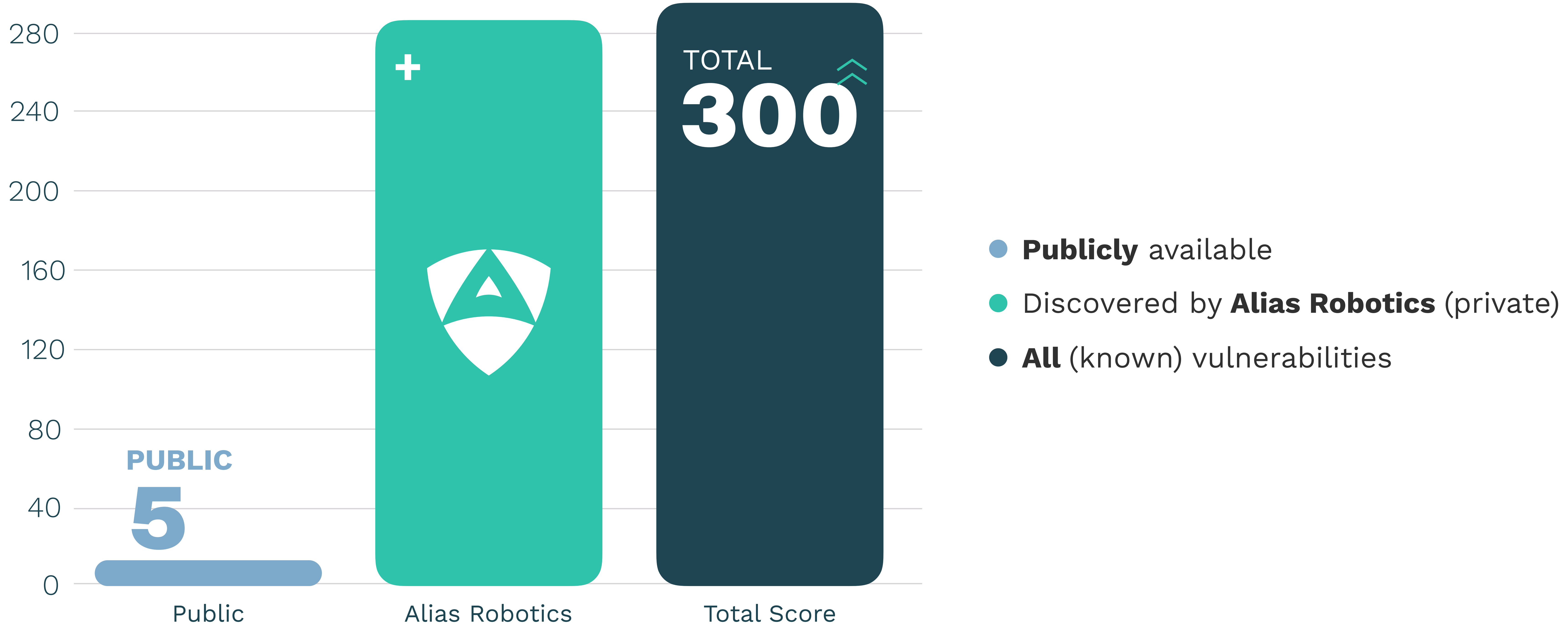

File
Program
Installation
Move
I/O
Log
10:31:22
CCCC
New Program
Load From File
Load Program
Use Template
Pick and Place
Empty Program
E-STOP
UNIVERSAL ROBOTS

alurity

ADDED VALUE OF ALIAS ROBOTICS

CASE OF STUDY

UNIVERSAL ROBOTS



DEFENSIVE
ROBOT SECURITY

ORIS

RIS

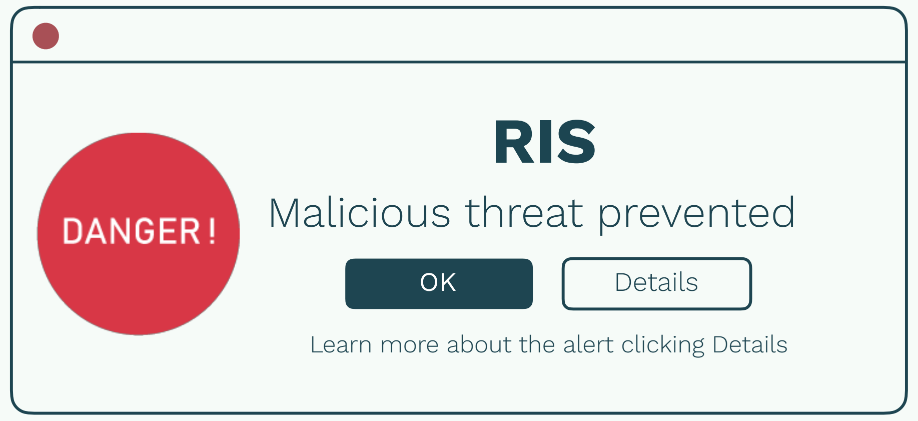
by ALIAS ROBOTICS

COMING SOON ›

INTRODUCING RIS
FOR UNIVERSAL ROBOTS

Hardens / Mitigates known vulnerabilities in Universal Robots

Alerts / Prevents of threats to Universal Robots



RIS

DANGER!

Malicious threat prevented

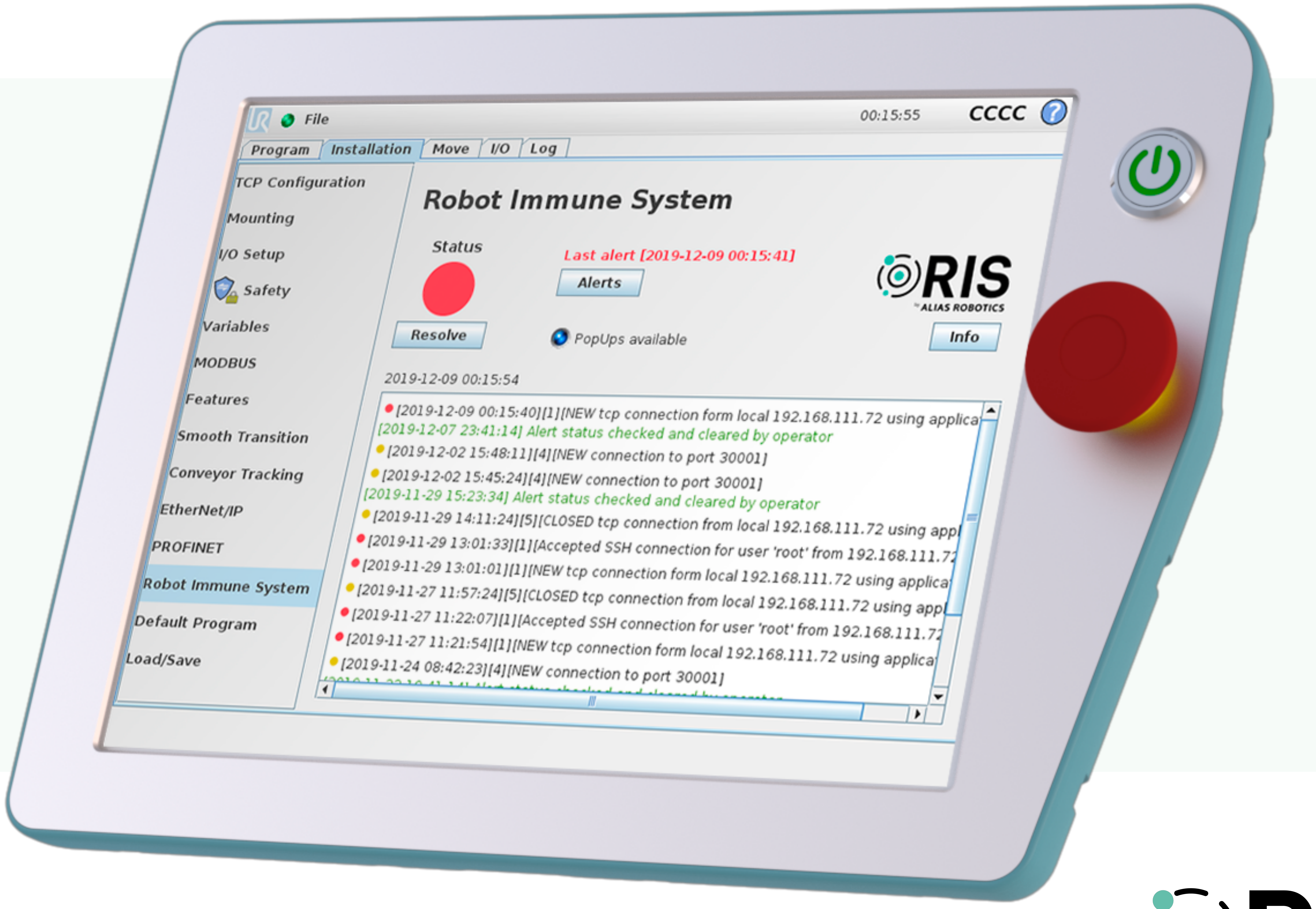
OK Details

Learn more about the alert clicking Details

● NORMAL No problem status

● WARNING! WARNING: Anomaly with potential threat to the system

● DANGER! DANGER: Dangerous action possibly compromising the system



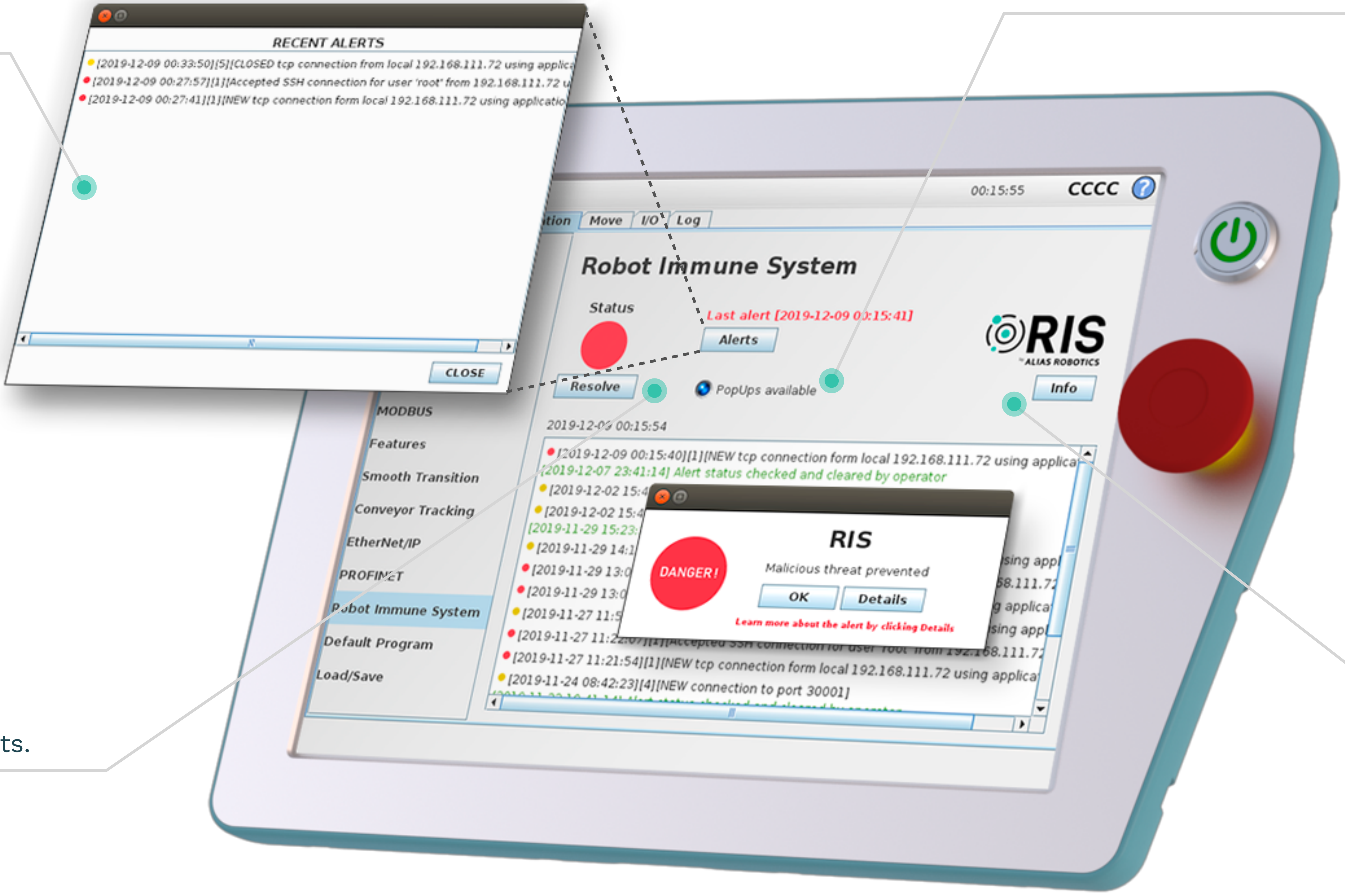
Robot Immune System

Last alert [2019-12-09 00:15:41]

2019-12-09 00:15:54

```
● [2019-12-09 00:15:40][1][NEW tcp connection form local 192.168.111.72 using applica
[2019-12-07 23:41:14] Alert status checked and cleared by operator
● [2019-12-02 15:48:11][4][NEW connection to port 30001]
● [2019-12-02 15:45:24][4][NEW connection to port 30001]
[2019-11-29 15:23:34] Alert status checked and cleared by operator
● [2019-11-29 14:11:24][5][CLOSED tcp connection from local 192.168.111.72 using appl
● [2019-11-29 13:01:33][1][Accepted SSH connection for user 'root' from 192.168.111.72
● [2019-11-29 13:01:01][1][NEW tcp connection form local 192.168.111.72 using applica
● [2019-11-27 11:57:24][5][CLOSED tcp connection from local 192.168.111.72 using appl
● [2019-11-27 11:22:07][1][Accepted SSH connection for user 'root' from 192.168.111.72
● [2019-11-27 11:21:54][1][NEW tcp connection form local 192.168.111.72 using applica
● [2019-11-24 08:42:23][4][NEW connection to port 30001]
```

INTRODUCING RIS
FOR UNIVERSAL ROBOTS



RECENT ALERTS

```
[2019-12-09 00:33:50][5][CLOSED tcp connection from local 192.168.111.72 using applica
[2019-12-09 00:27:57][1][Accepted SSH connection for user 'root' from 192.168.111.72 u
[2019-12-09 00:27:41][1][NEW tcp connection form local 192.168.111.72 using applicatio
```

Robot Immune System

Last alert [2019-12-09 00:15:41]

PopUps available

2019-12-09 00:15:54

```
[2019-12-09 00:15:40][1][NEW tcp connection form local 192.168.111.72 using applica
[2019-12-07 23:41:14] Alert status checked and cleared by operator
[2019-12-02 15:4
[2019-12-02 15:4
[2019-11-29 15:23:
[2019-11-29 14:1
[2019-11-29 13:0
[2019-11-29 13:0
[2019-11-27 11:5
[2019-11-27 11:22:07][1][Accepted SSH connection for user 'root' from 192.168.111.72
[2019-11-27 11:21:54][1][NEW tcp connection form local 192.168.111.72 using applica
[2019-11-24 08:42:23][4][NEW connection to port 30001]
```

RIS

DANGER!

Malicious threat prevented

Learn more about the alert by clicking Details

Check your UR robot's last alerts. It shows all recent Danger or Warning alerts that have not been checked.

Enable or disable alert Popups. Activate it if you want to receive notifications when alerts occur.

Contains information about RIS operation. Come here whenever you need help.

Reset to a no problem status when you have already checked your alerts.

RIS

MOTIVATION
ROBOT SECURITY SURVEY

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”

- Upon PoC attack “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 ”

A SNEAK PEAK INTO ROBOT SECURITY SURVEY

ROBOT SECURITY **SURVEY**

ALIAS ROBOTICS
Robot Cybersecurity

JOANNEUM RESEARCH ROBOTICS

OBJECTIVE

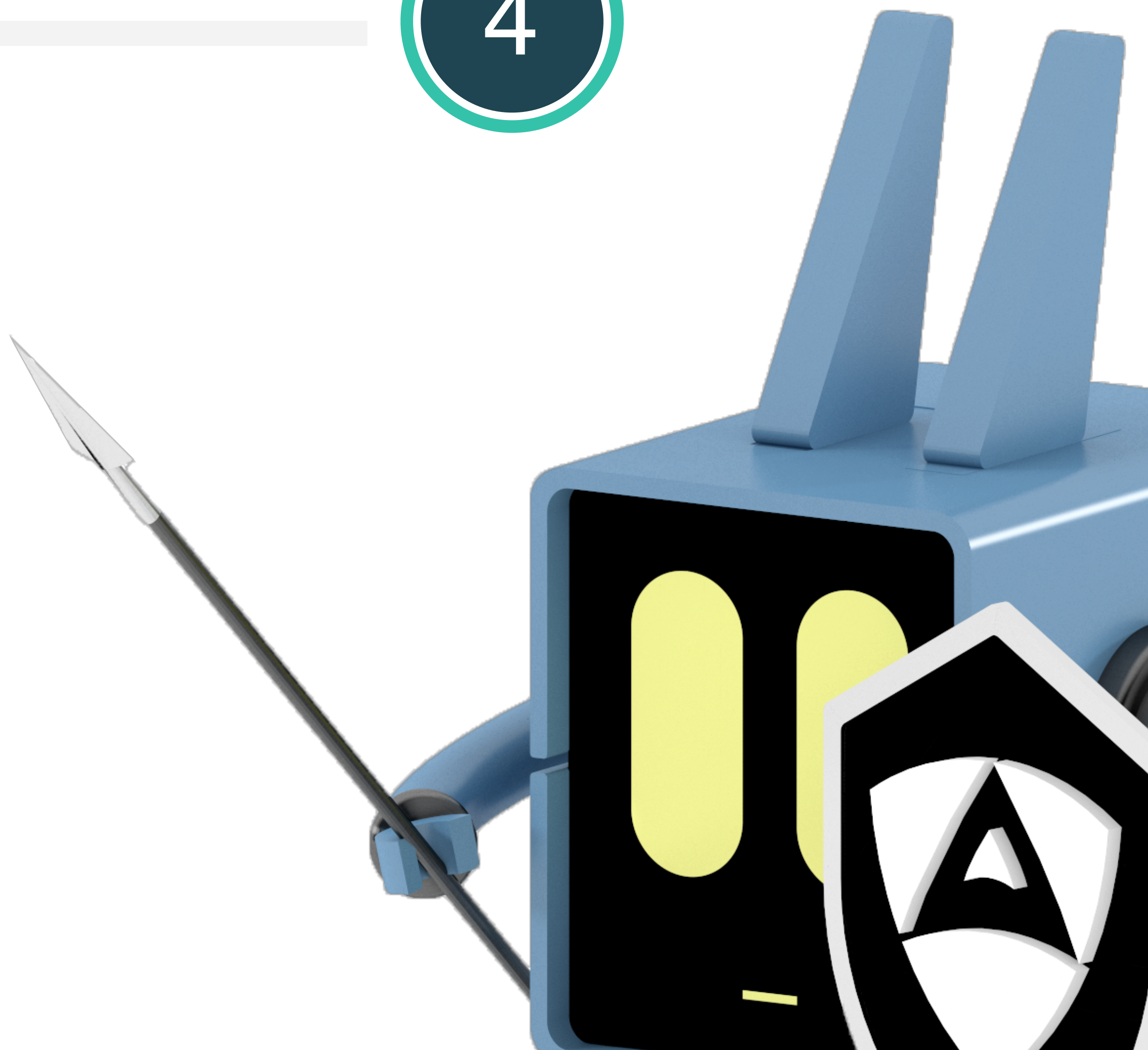
Depict a global landscape of the current security situation in robotics.

RATIONALE

The need to assess precisely the security concerns in **the robotics value chain** and the strategies of cybersecurity so far.

STRUCTURE
ROBOT SECURITY SURVEY

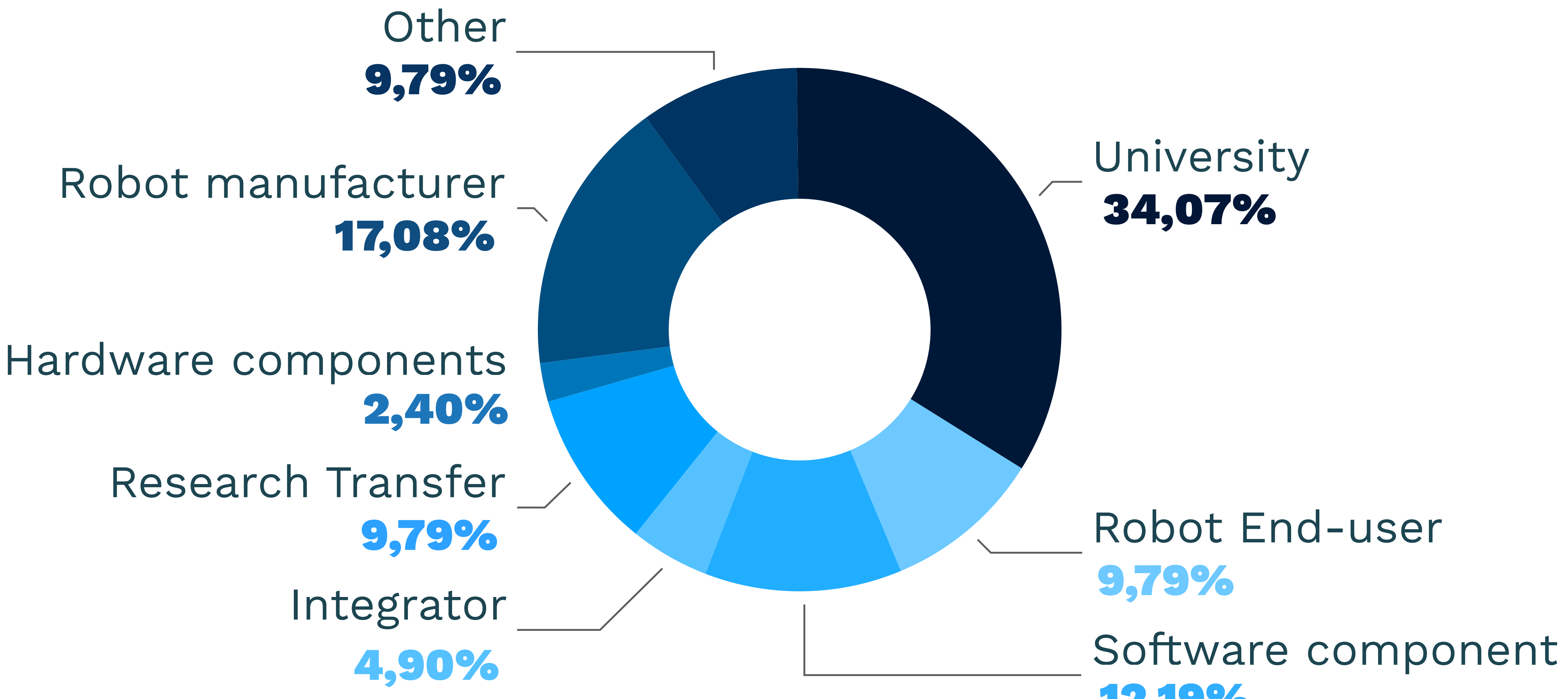
1. General **Questions** and background
2. Robot **usage** and **application**
3. Cybersecurity **specifics**
4. **Standardization** Items



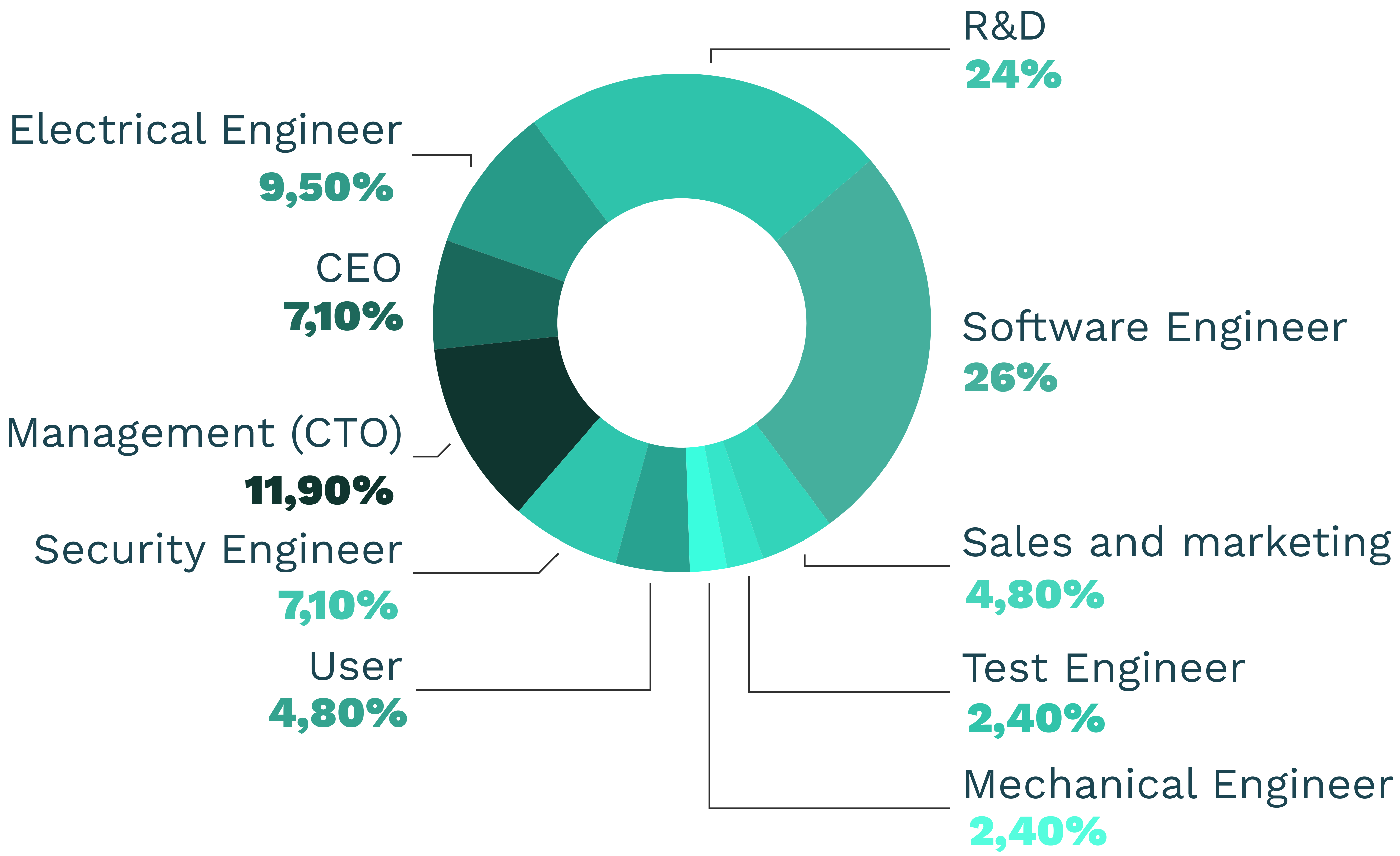
RESPONDANT PROFILES

43 RESPONSES
AT TIME OF WRITING

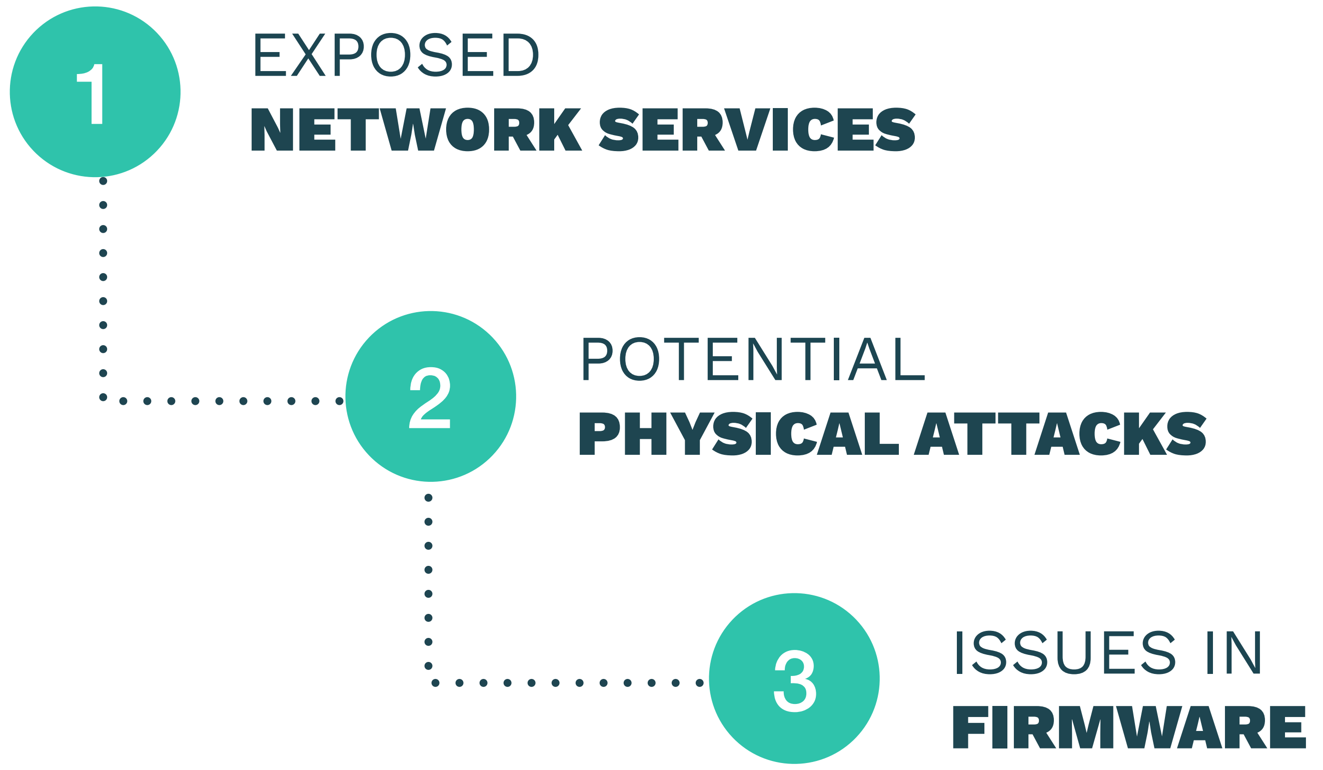
RESPONDANT **PROFILES**



VARIOUS **BACKGROUNDS & POSITIONS**



(IN)SECURITY
OBSERVATIONS



1 EXPOSED **NETWORK SERVICES**

2 POTENTIAL **PHYSICAL ATTACKS**

3 ISSUES IN **FIRMWARE**

51%

IDENTIFIED
CYBER - WEAKNESSES IN ROBOTS

9%

WITNESSED
A CYBERATTACK

SUSPECTED/OBSERVED
VULNERABILITIES

(IN)SECURITY CONCERNS

RESPONDENT FEARS

1st	IP STEALING
2nd	SAFETY VIOLATIONS

OUTCOME LIKELIHOOD

1st	SAFETY VIOLATIONS
2nd	DATA LOSS

MALICIOUS ACTORS

1st	HACKERS
2nd	UNINTENTIONAL EMPLOYEES

SECURITY PERCEPTION

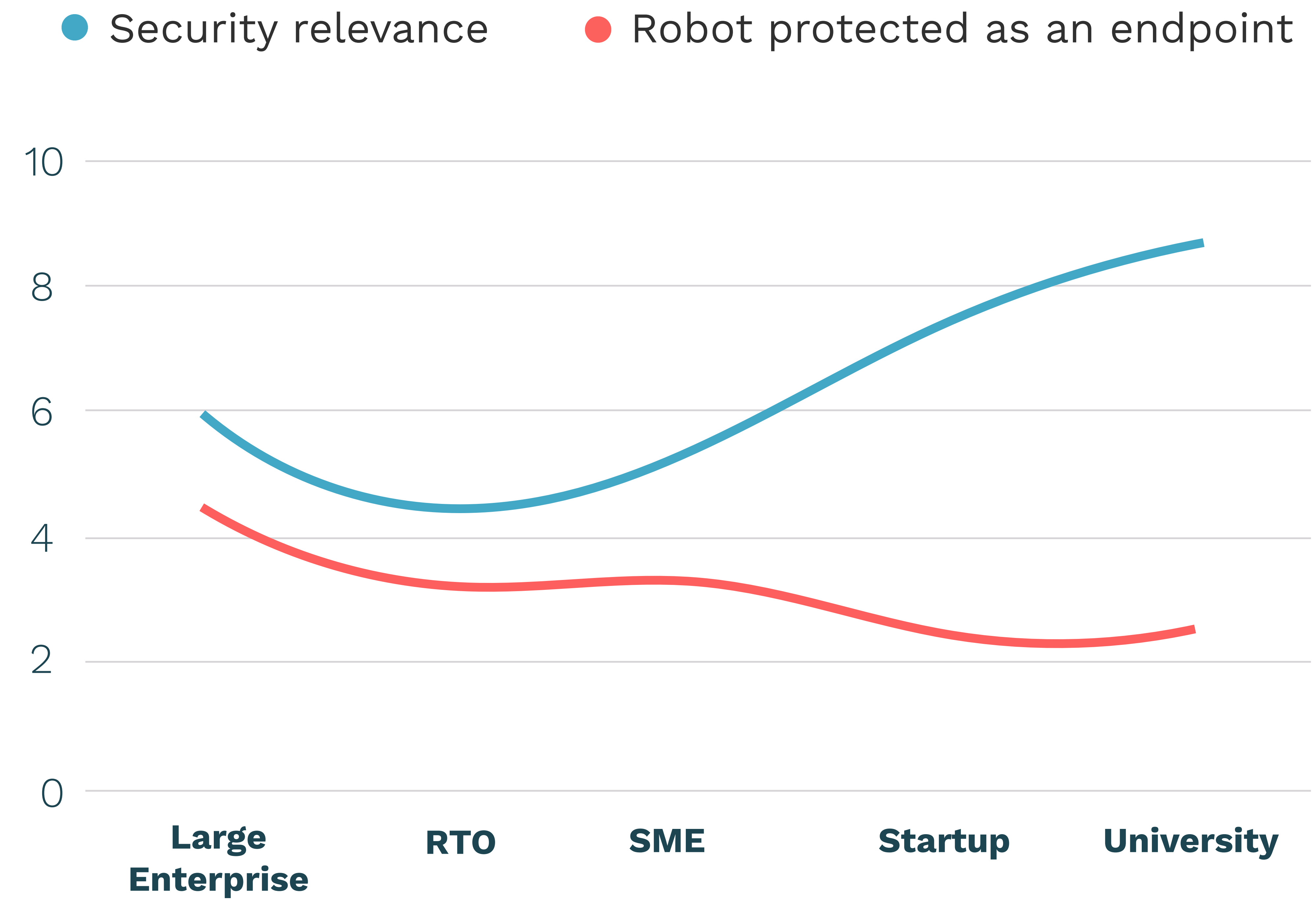
8/10

SECURITY RELEVANCE

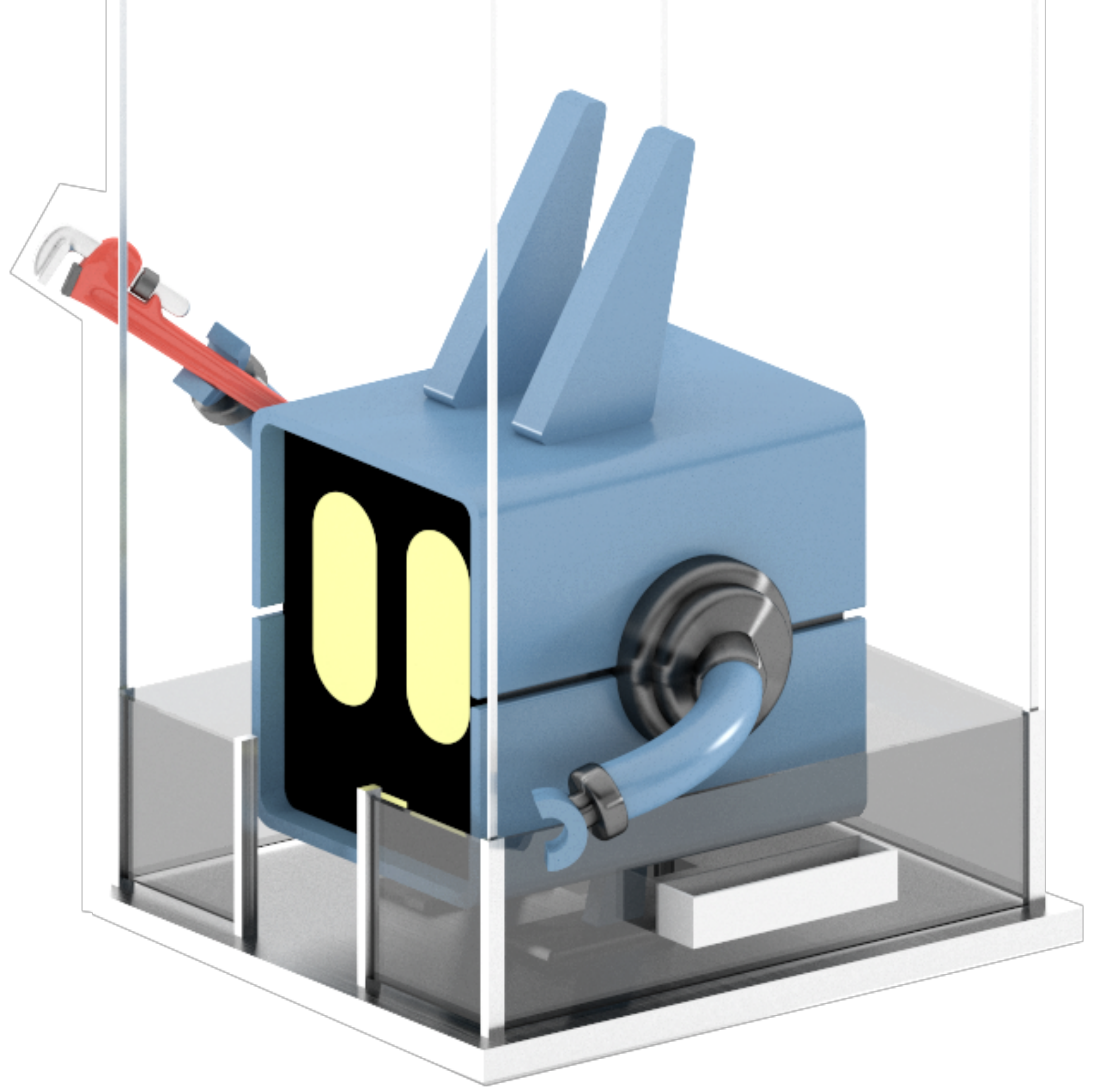
2.2/10

PROTECTED **AS AN ENDPOINT?**

UNSTACKED
RELEVANCE & ENDPOINT SECURITY



ECONOMIC CONSIDERATIONS



73%

OPEN TO INVEST

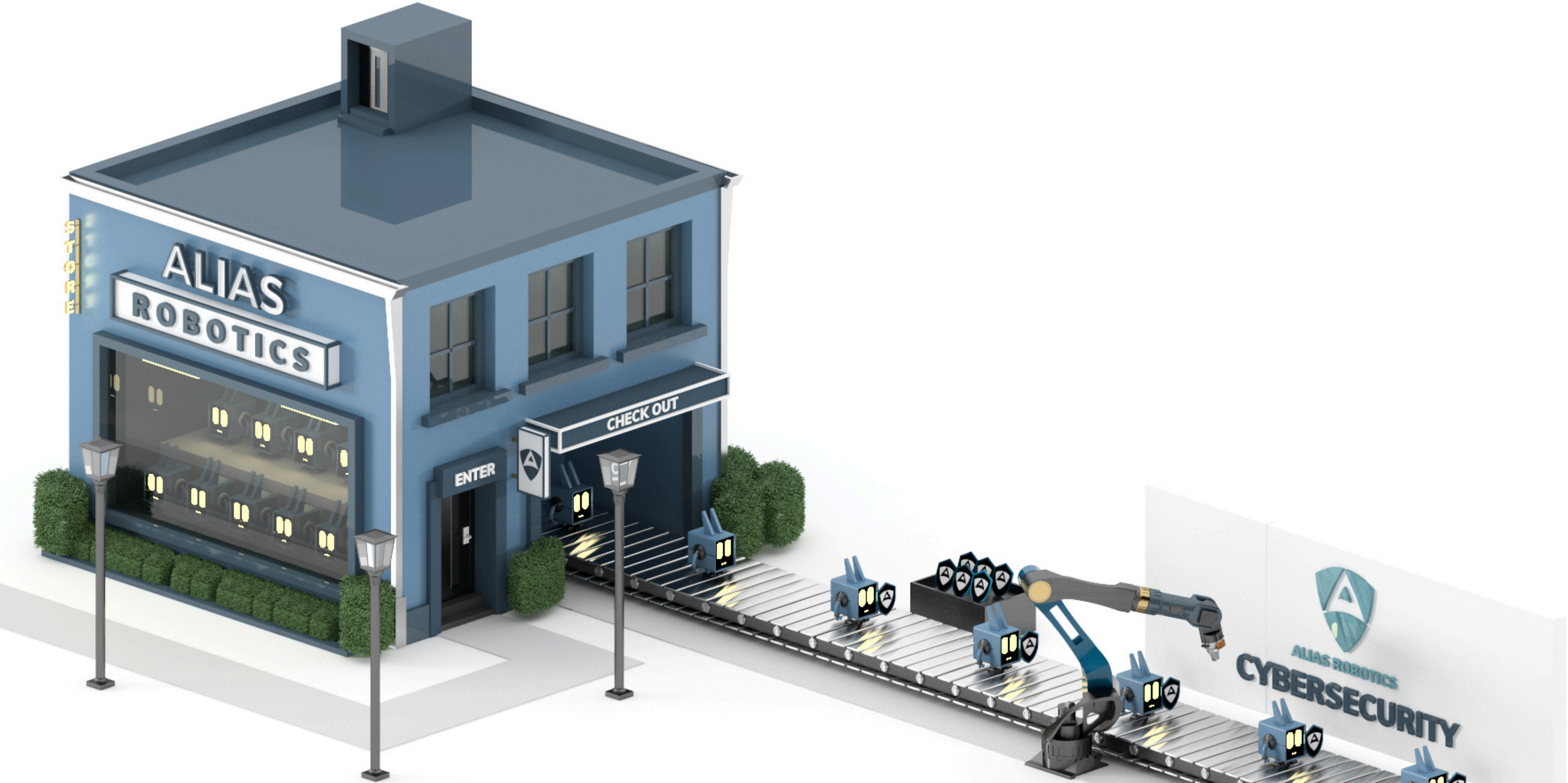
26%

HAVE ACTUALLY **INVESTED**

73%

THINK THEY HAVE NOT **INVESTED ENOUGH**

CALL FOR ACTION



REMOVING 0-DAYS

FROM ROBOTICS

ALIAS ROBOTICS
Robot Cybersecurity

www.**aliasrobotics**.com

contact@aliasrobotics.com