SECURITY IN ROS & ROS 2

ROBOT SETUPS

ALIAS ROBOTICS

Robot Cybersecurity

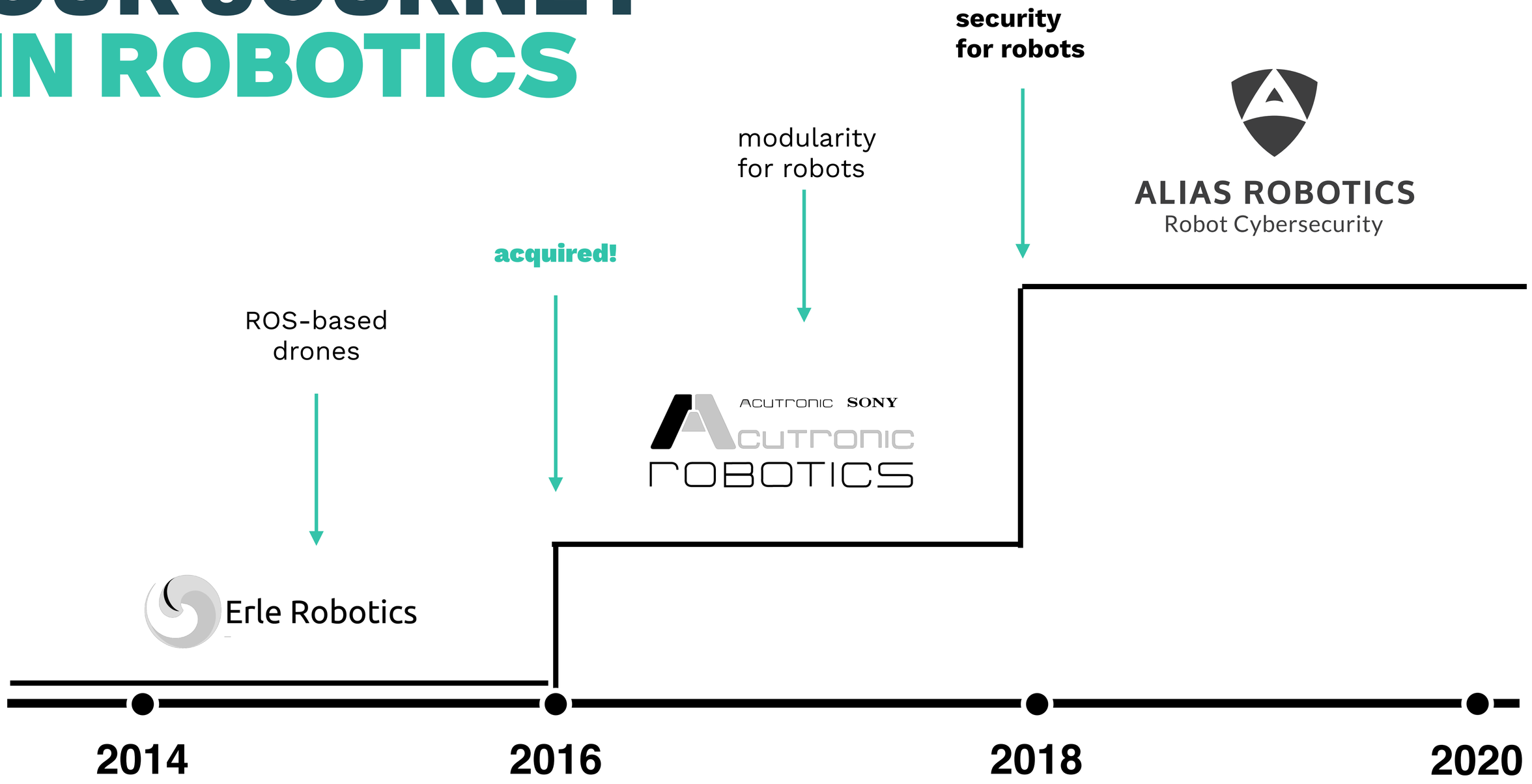
VÍCTOR MAYORAL VILCHES

victor@aliasrobotics.com

ALIAS ROBOTICS

Alias Robotics is a robot cyber security firm. Founded upon previous experiences in robotics, we take a roboticists' approach to cyber security and deliver security solutions for robots and their components.

OUR JOURNEY IN ROBOTICS



CONTACT US
OUR LOCATIONS

2018
SPAIN, VITORIA

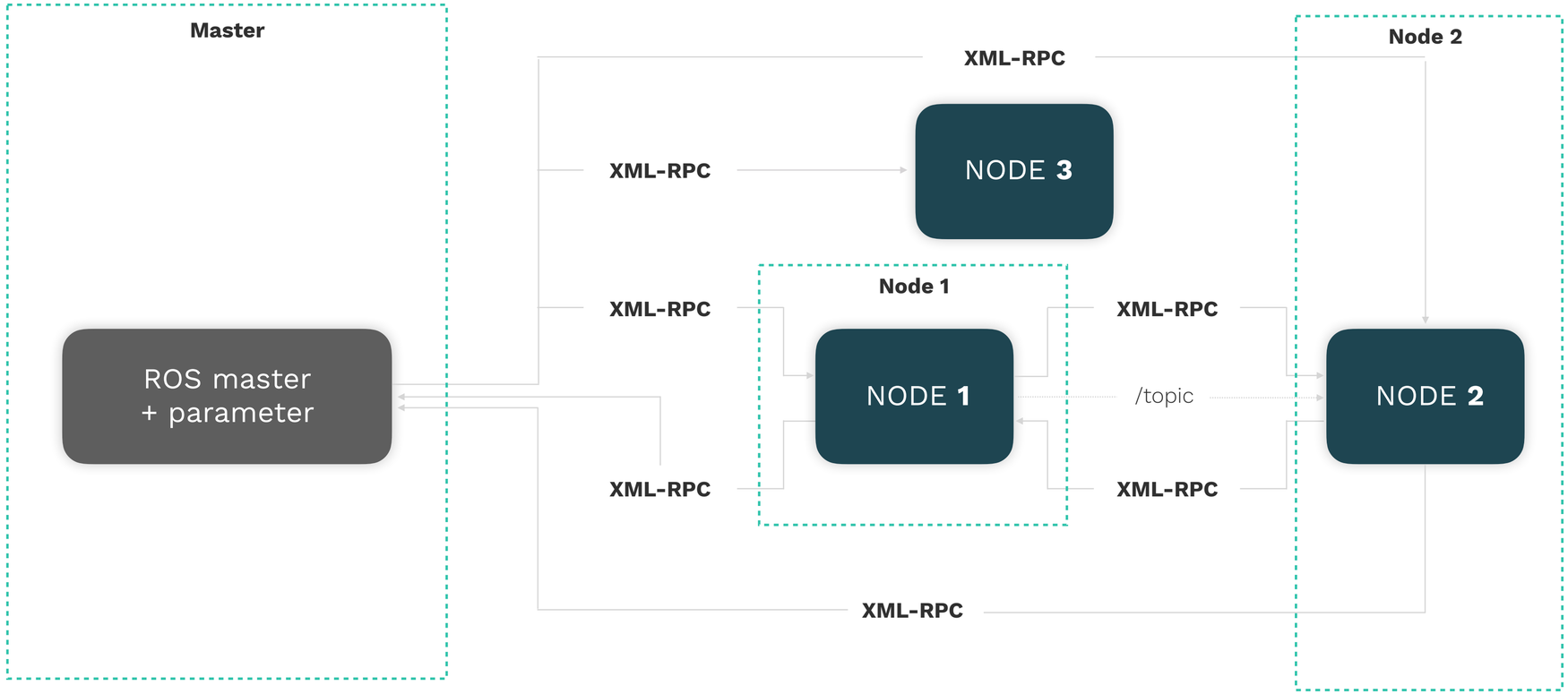
2020
BOSTON, MA

ROS
SECURITY

QUICK REVIEW

COMPUTATIONAL GRAPH OF **ROS1**

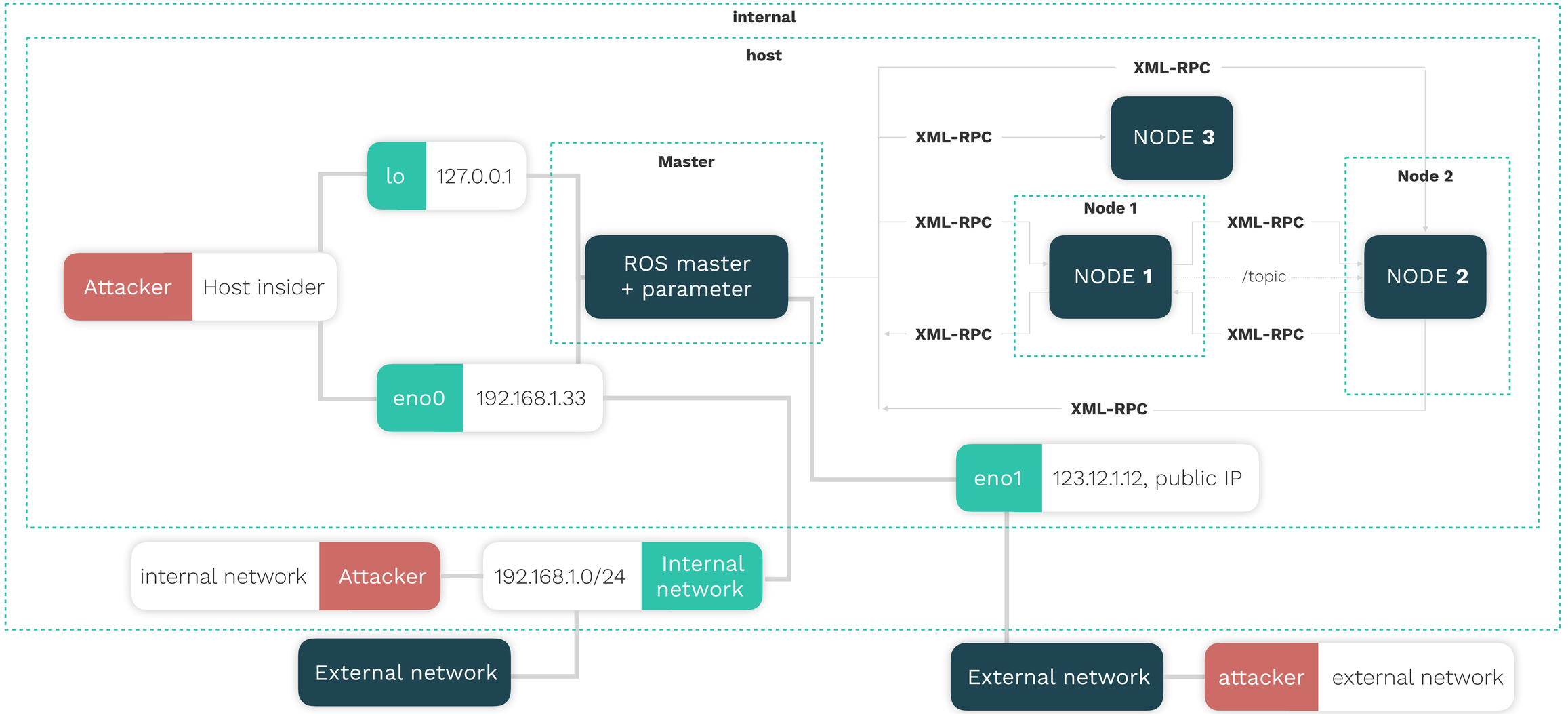
The **computational graph** models the computational nodes with their topics, services and other abstractions.



QUICK REVIEW

DATA LAYER GRAPH OF **ROS**

The **data layer graph** represents the physical groupings and connections which implement the behavior modeled in the *computational graph*



RECONNAISSANCE
RESULTS FOR ROS 1

TABLE 1: SCAN RESULTS FOR ROS SYSTEMS BY COUNTRY

	SCAN 1				SCAN 2			
COUNTRY	EMPTY	REAL	SIMULATION	**TOTAL**	EMPTY	REAL	SIMULATION	**TOTAL**
AU	0	1	0	**1**	0	1	0	**1**
CA	4	1	0	**5**	0	1	1	**2**
CN	2	0	0	**2**	3	2	2	**7**
CZ	0	0	0	**0**	2	0	0	**2**
DE	0	0	0	**0**	1	0	1	**2**
ES	1	0	0	**1**	4	0	0	**4**
EU	0	0	0	**0**	0	1	0	**1**
GR	0	0	0	**0**	1	4	0	**5**
HK	2	2	0	**4**	2	0	0	**2**
IT	1	0	0	**1**	4	1	0	**5**
JP	2	0	0	**2**	1	0	0	**1**
KR	5	0	3	**8**	6	4	6	**16**
NL	1	0	0	**1**	1	0	0	**1**
SE	1	0	0	**1**	0	0	0	**0**
SG	0	0	0	**0**	1	0	0	**1**
TW	2	0	0	**2**	2	0	2	**4**
US	21	7	0	**28**	25	22	5	**52**
GRAND TOTAL	**42**	**11**	**3**	**56**	**53**	**36**	**17**	**106**

EXAMPLE OF INDUSTRIAL TRASH CLASSIFICATION ROBOT **FOUND WITH AZTARNA**

zmap -p 11311 0.0.0.0/0 -q | aztarna -t ROS -p 11311

Vilches, V. M., Mendia, G. O., Baskaran, X. P., Cordero, A. H., Juan, L. U. S., Gil-Uriarte, E., ... & Kirschgens, L. A. (2018).
aztarna, a footprinting tool for robots.
arXiv preprint arXiv:1812.09490.

N. DeMarinis, S. Tellex, V. Kemerlis, G. Konidaris, and R. Fonseca,
“Scanning the Internet for ROS:A View of Security in Robotics Research,”
2018.

ROSin

This repository was partly funded by ROSIN RedROS2-I FTP which received funding from the European Union’s Horizon 2020 research and innovation programme under the project ROSIN with the grant agreement No 732287.

EXAMPLE OF INDUSTRIAL TRASH CLASSIFICATION ROBOT **FOUND WITH AZTARNA**

zmap -p 11311 0.0.0.0/0 -q | aztarna -t ROS -p 11311

Vilches, V. M., Mendia, G. O., Baskaran, X. P., Cordero, A. H., Juan, L. U. S., Gil-Uriarte, E., ... & Kirschgens, L. A. (2018).
aztarna, a footprinting tool for robots.
arXiv preprint arXiv:1812.09490.

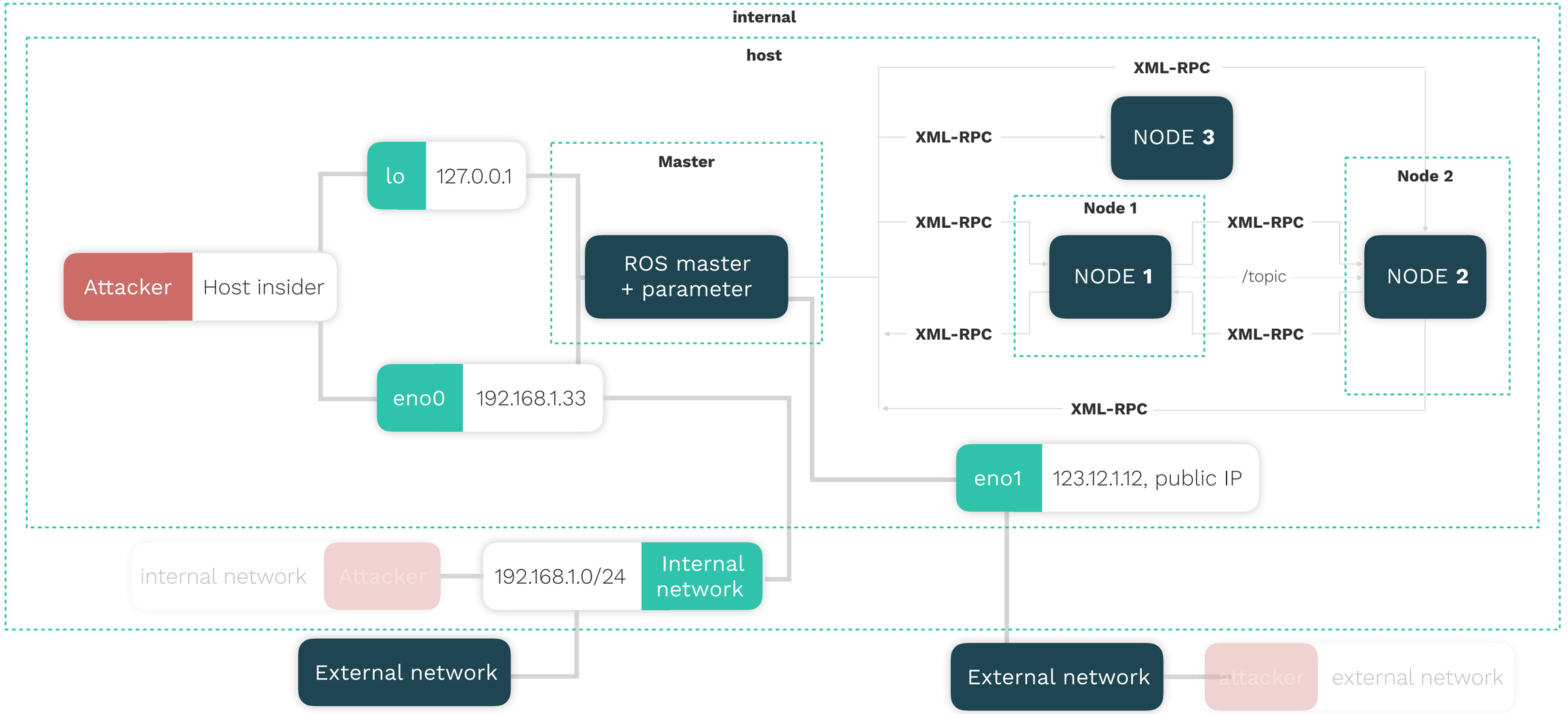
N. DeMarinis, S. Tellex, V. Kemerlis, G. Konidaris, and R. Fonseca,
"Scanning the Internet for ROS:A View of Security in Robotics Research,"
2018.

This repository was partly funded by ROSIN RedROS2-I FTP which received funding from the European Union's Horizon 2020 research and innovation programme under the project ROSIN with the grant agreement No 732287.

APPLYING MITIGATIONS: SROS

COMMUNICATION SECURITY

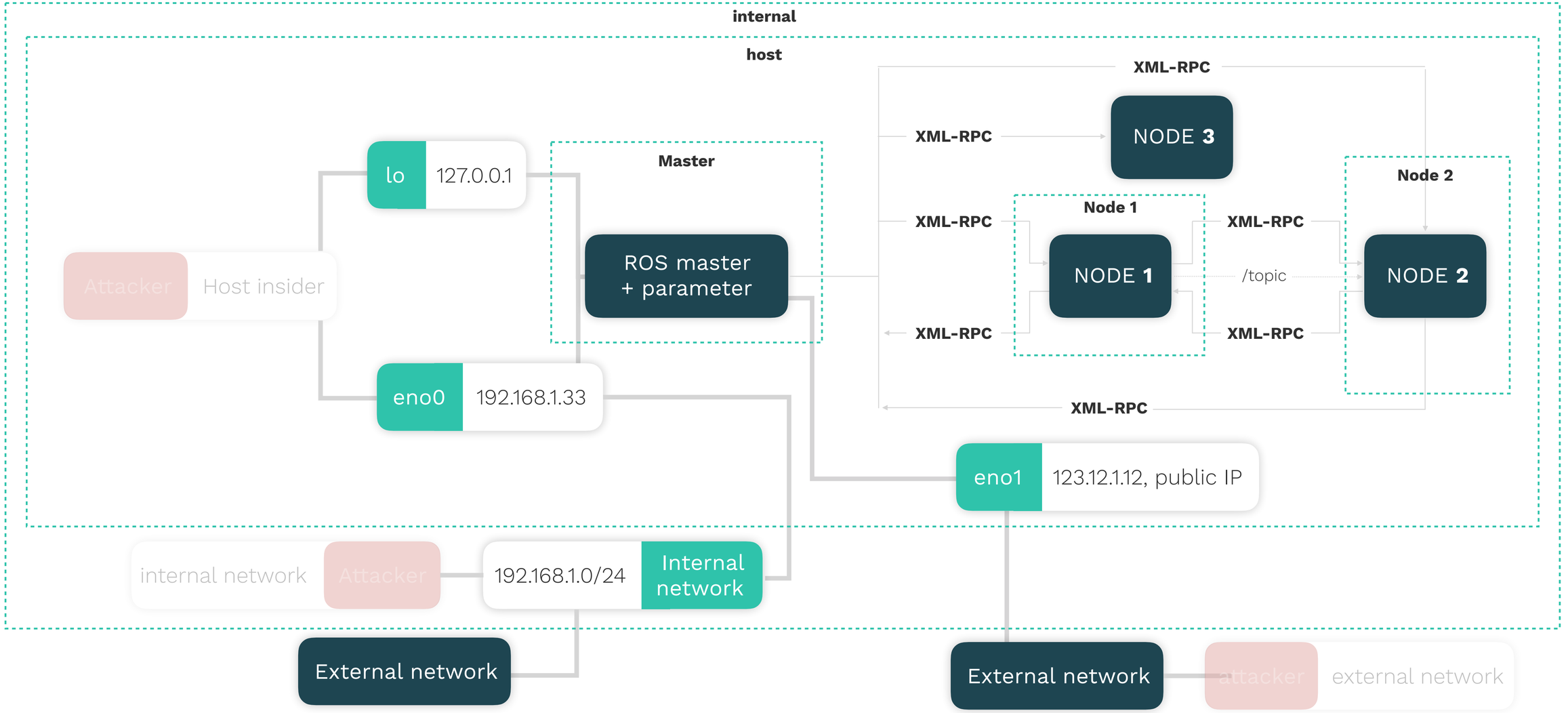
related to protecting communications (COMMUNICATION SECURITY, also known as COMSEC)



APPLYING MORE MITIGATIONS: APPARMOR

SYSTEMS SECURITY

concerned with protecting one's machines and data. The intent is that machines should be used only by authorized users and for the purposes that the owners intend.



ARE WE THEN SECURE IN ROS SYSTEMS?

NO, WE AREN'T

>_some reasoning X

```
# A number of issues with SROS
  - Only “some" support in Kinetic (not in Melodic)
  - No active maintainer
  - Not that easy to maintain
  - Needs still lots of (security) testing to be bug-free

# A number of issues with AppArmor
  - Very few known use cases in robotics employing
  - Not that easy to maintain (though much easier than other
alternatives, e.g. SELinux)
```

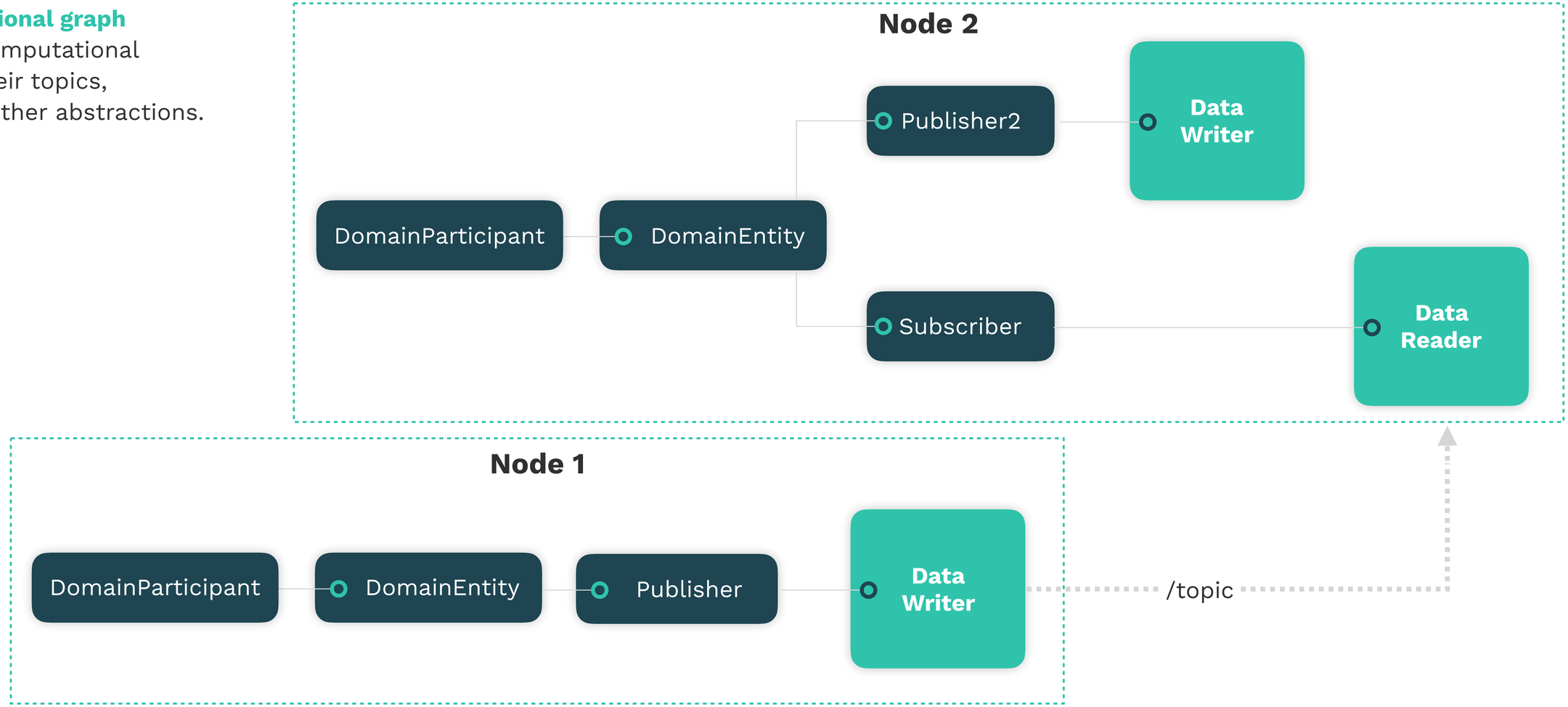
SECURITY ADVICE?

MOVE TO ROS 2, BUT IS THAT ENOUGH?

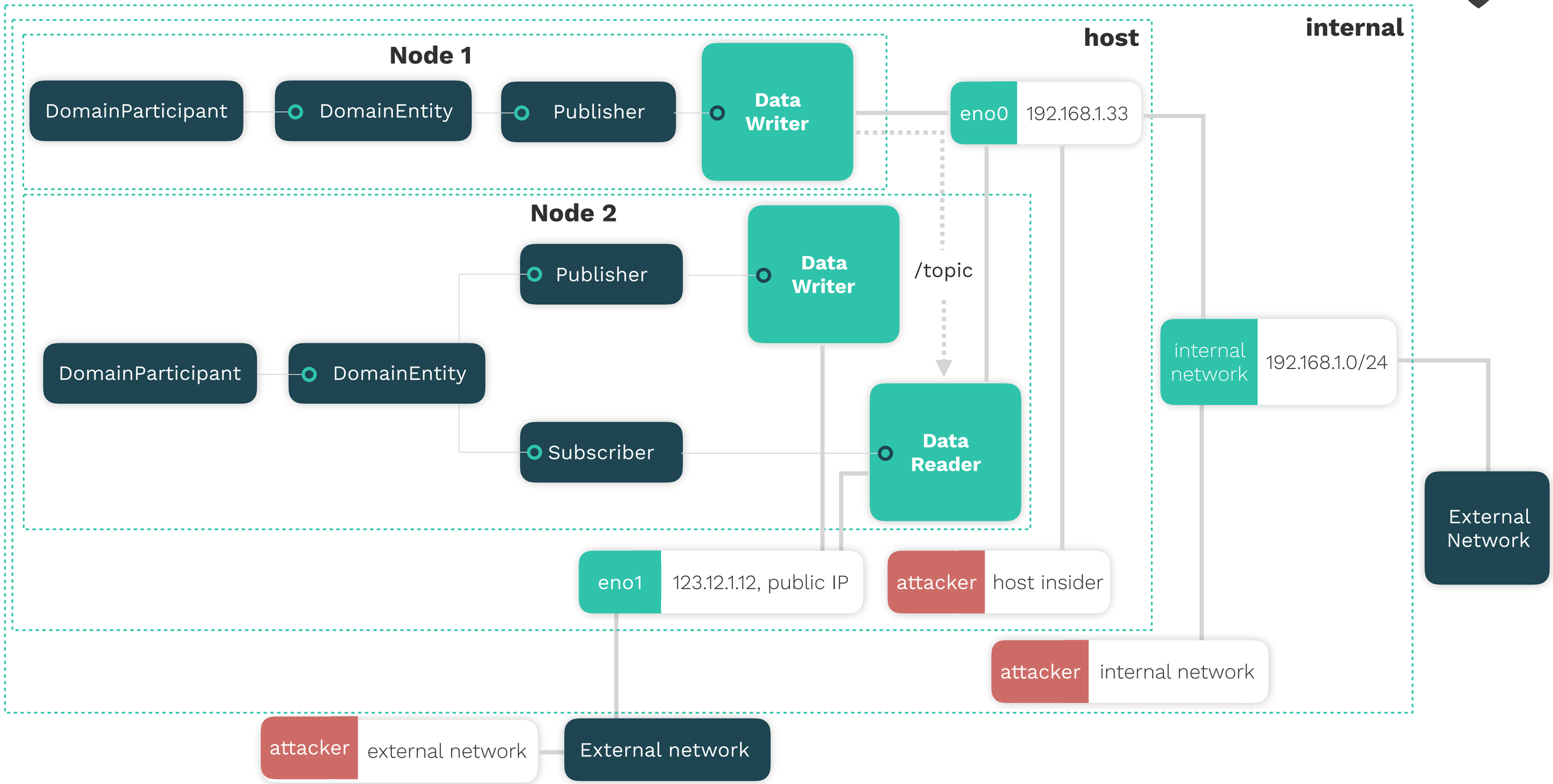
ROS 2
SECURITY

COMPUTATIONAL GRAPH OF **ROS2**

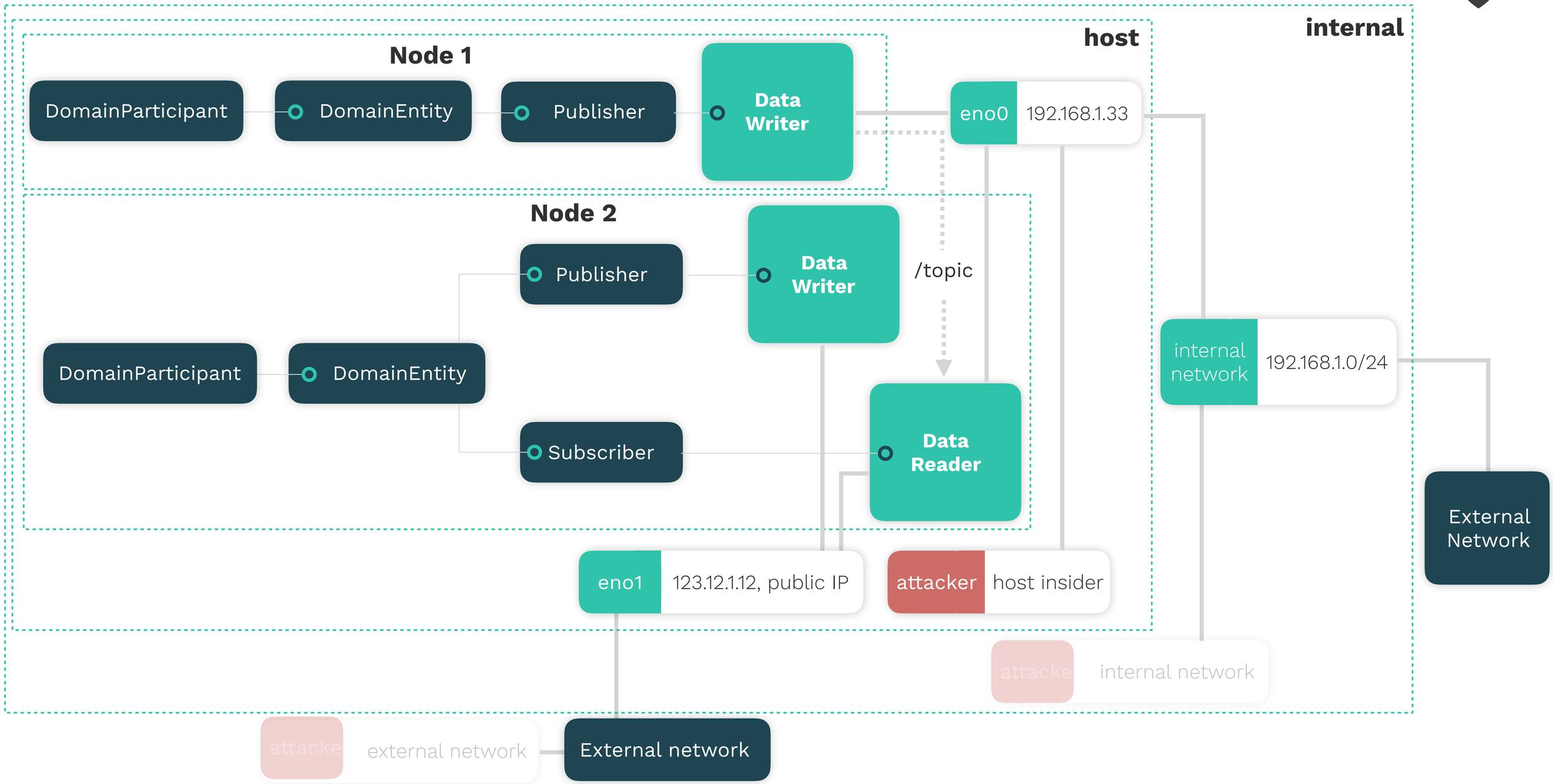
The **computational graph** models the computational nodes with their topics, services and other abstractions.



DATA LAYER GRAPH OF **ROS 2**



APPLYING MITIGATIONS: SROS2



ARE WE THEN SECURE IN ROS 2 SYSTEMS?

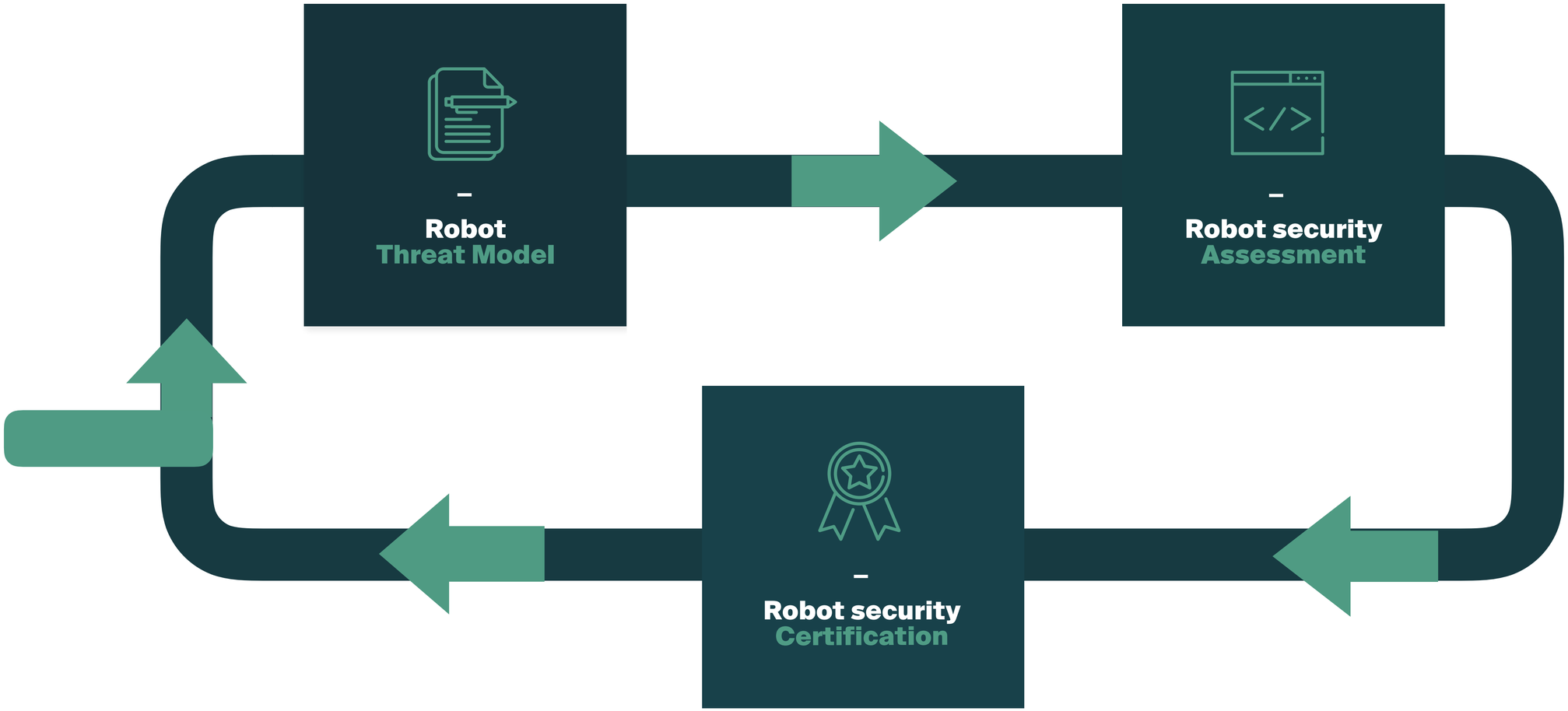
NO, WE AREN'T

```
>_some reasoning                                                    X

# A number of issues with SROS2
  - Limited functionality with some DDS implementations, proper
security (and security interoperability) testing needs to happen
  - Rapidly changing to overcome some DoS threats
  - Being developed/maintained by volunteers
  - Subject to reconnaissance attacks due to the nature of
dynamic discovery in DDS

# No known (and open) systems security solution adapted/used with
ROS2
```

SECURITY ADVICE?

INVEST PROACTIVELY IN SECURITY, BUILD A SECURITY TEAM AND REQUEST EXTERNAL HELP

THE IDEAL
SECURITY FLOW



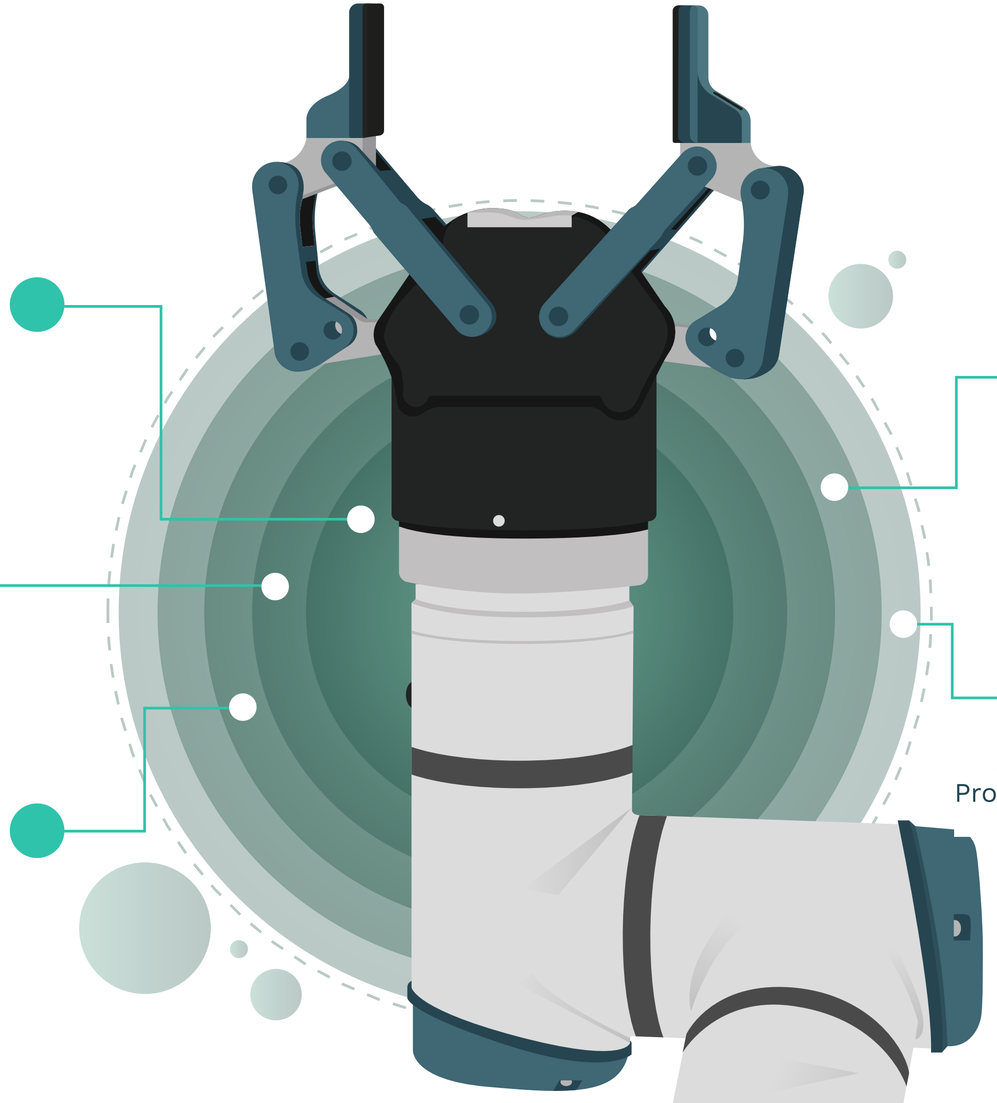
RIS

by ALIAS ROBOTICS

ROBOT IMMUNE SYSTEM

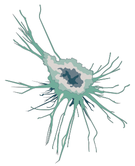
Robot cyberattacks & malfunctions

RIS
ENDPOINT-PROTECTION



SKIN
Firewall

Preliminary filters. Re-configures depending on the environment.



INNATE IMMUNITY
Hardening

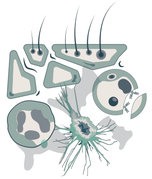
Fixes security flaws. Provides generic defense.

MEMORY
Logging

Provides a record of traceability

ADAPTATIVE IMMUNE SYSTEM
AI

Provides a learning framework for RIS



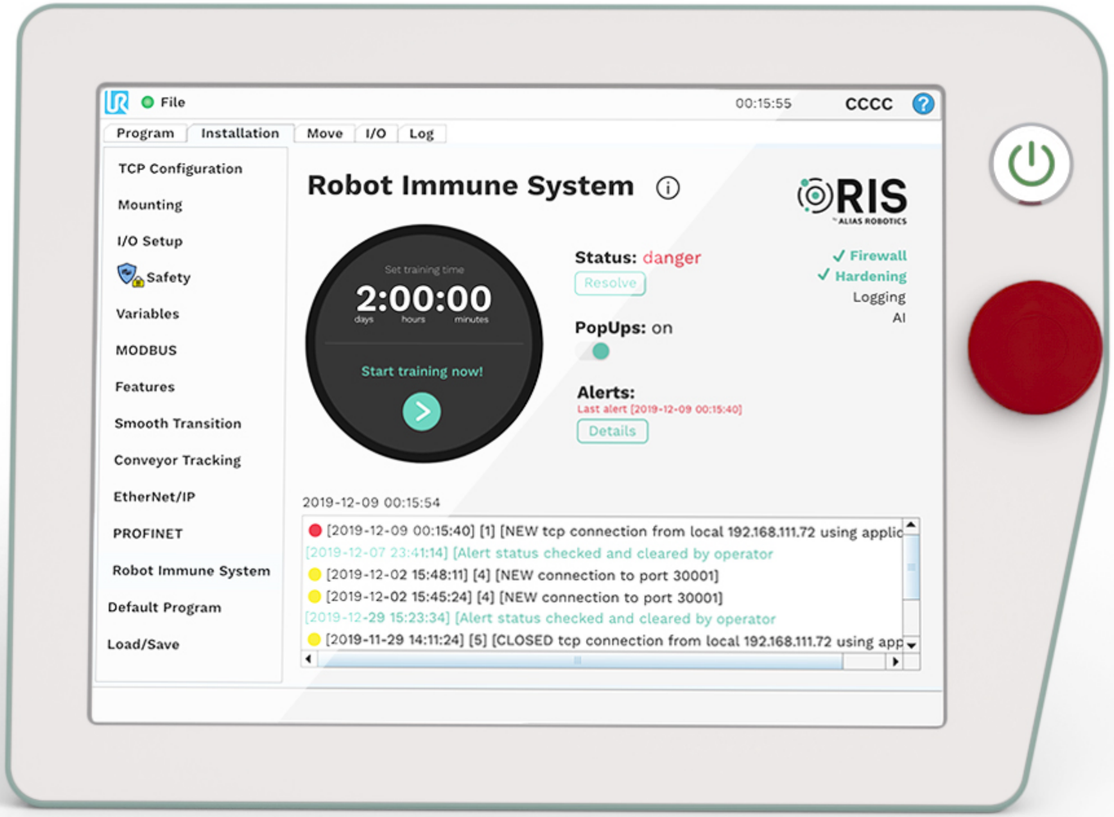
A HOLISTIC VIEW
Visualization

Analytics of the biological visualization. Provides visualization and analytics of RIS.

HOW DOES IT WORK

Its modular architecture allows us to embed the Robot Immune System (RIS) directly into the robot putting together **anti-virus solution for robots**.

Currently RIS supports ROS, ROS 2 and UR robots (UR3, UR5, UR10)



UR3 UR5 UR10 2 ROS

REMOVING 0-DAYS

FROM ROBOTICS

ALIAS ROBOTICS

Robot Cybersecurity

www.**aliasrobotics**.com

contact@aliasrobotics.com