

FORESIGHT project: Concept, objectives and current progress

Advanced cyber-security simulation platform for preparedness training in Aviation, Naval and Power-grid environments

Prof. Nicholas E. Kolokotronis, *Technical Coordinator*

University of the Peloponnese (UOP)
Department of Informatics and Telecommunications

Cyber-Security challenges and future perspectives | Webinar

18/01/2022



This project has received funding from the European Union's Horizon 2020 Research and Innovation Action under Grant Agreement No 833673.



Partners

Project Coordinator



10.2019 – 03.2023

- 22 partners
- 9 EU M. States
- Budget 6 M

Project Partners



MINDS & SPARKS



AIRBUS



10.2019 – 03.2023

- 22 partners
- 9 EU M. States
- Budget 6 M

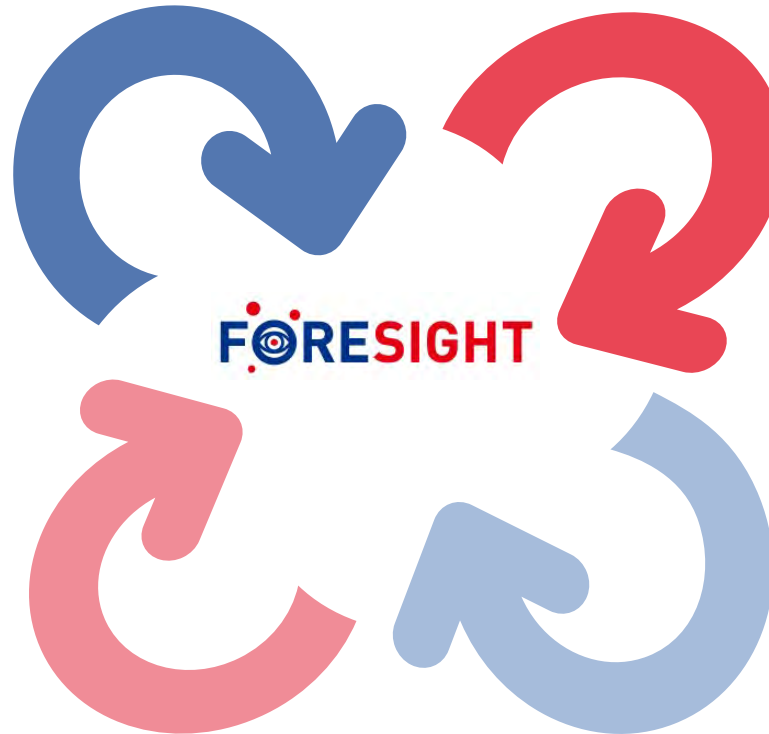


THALES



FORESIGHT motivation

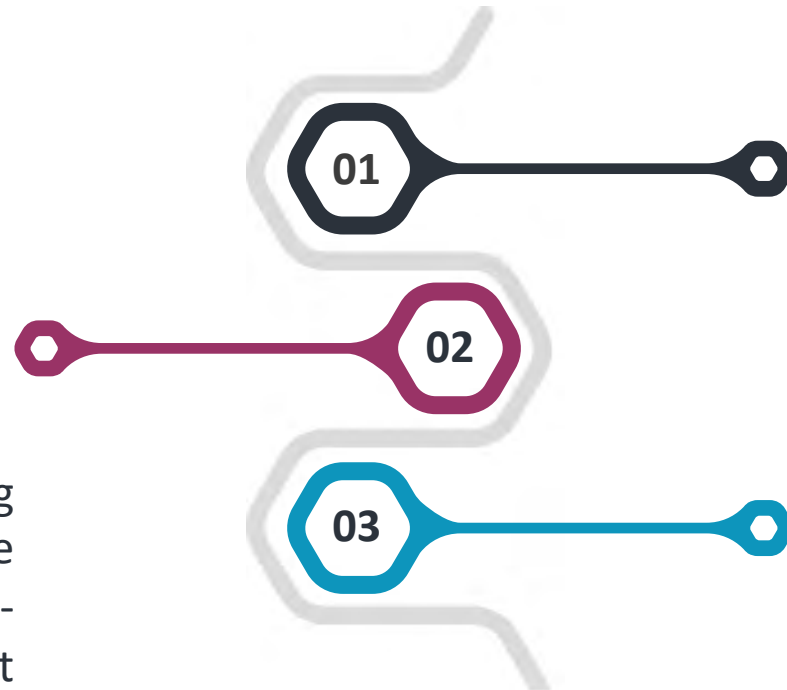
- ✓ Rapid growth of new forms of cyber-attacks that are quite hard to forecast, detect, mitigate, but also to recover
- ✓ The need for the development of innovative ways to implement security measures
- ✓ Security technology market fragmentation in cyber-defense systems
- ✓ Security skills' shortage
- ✓ Lack of security executives' deep awareness of cyber-security risks



- ✓ Highly skilled cyber-security professionals are needed by the industry
- ✓ Cyber security training should be a continuous learning process
- ✓ Advancements in realistic, diverse, and dynamic simulation environments

complex cross domain/hybrid scenarios

Extend the capabilities of existing cyber-ranges and will allow the creation of complex cross-domain/hybrid scenarios to be built jointly with the IoT domain



Federated cyber range

Develop a federated cyber-range solution to enhance the preparedness of cybersecurity professionals at all levels and advance their skills towards preventing, detecting, reacting and mitigating sophisticated cyberattacks

ecosystem of networked realistic training and simulation platforms

Deliver an ecosystem of networked realistic training and simulation platforms that collaboratively bring unique cybersecurity aspects from the aviation, smart grid and naval domains



CREATE a state-of-the art platform that will greatly extend the capabilities of existing cyber-ranges by allowing them to be a part of a cyber-range federation.



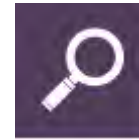
DELIVER training curricula aimed at cyber-security professionals to implement and combine security measures in innovative ways.



DEVELOP realistic and dynamic scenarios based on identified and forecasted trends and needs in terms of cyber-attacks and vulnerabilities.



INCREASE the dynamics of training and awareness methods in order to match or even exceed the rate of evolution of cyber-attackers.



IDENTIFY the impact of cyber-risks and the most appropriate security measures to protect valuable assets, minimise costs and recovery time.



IMPROVE the number of talented cyber-security professionals to meet the industry's current needs at all levels (from junior to senior).

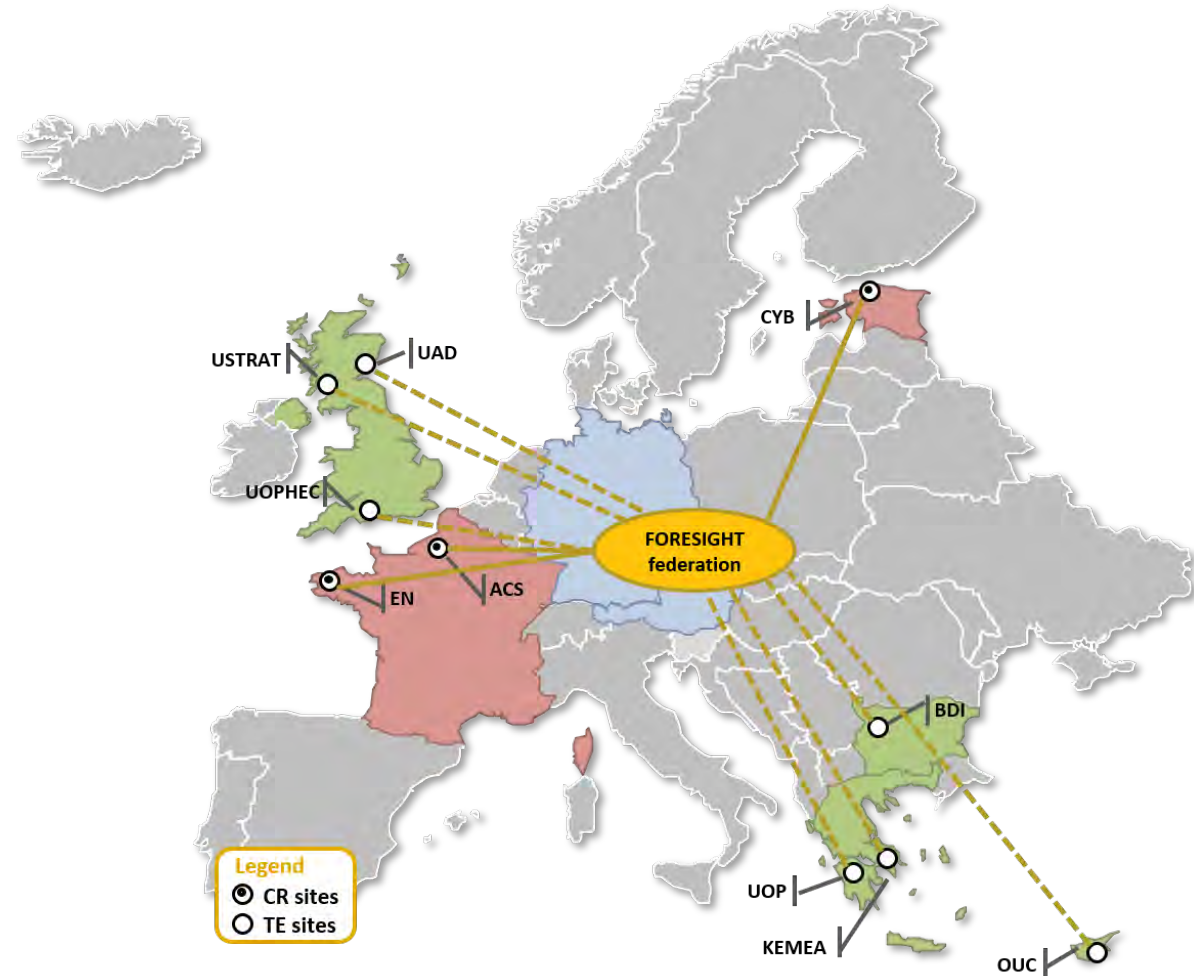
FORESIGHT federation platform for CRs/TEs

FORESIGHT CRs:

- 3 different Cyber Ranges from two different countries:
CybExer from Estonia, **Airbus** and the **French Naval Academy** from France.
- Developed for different domains but provide training regarding cyber security preparedness and incident response to cyber security experts.

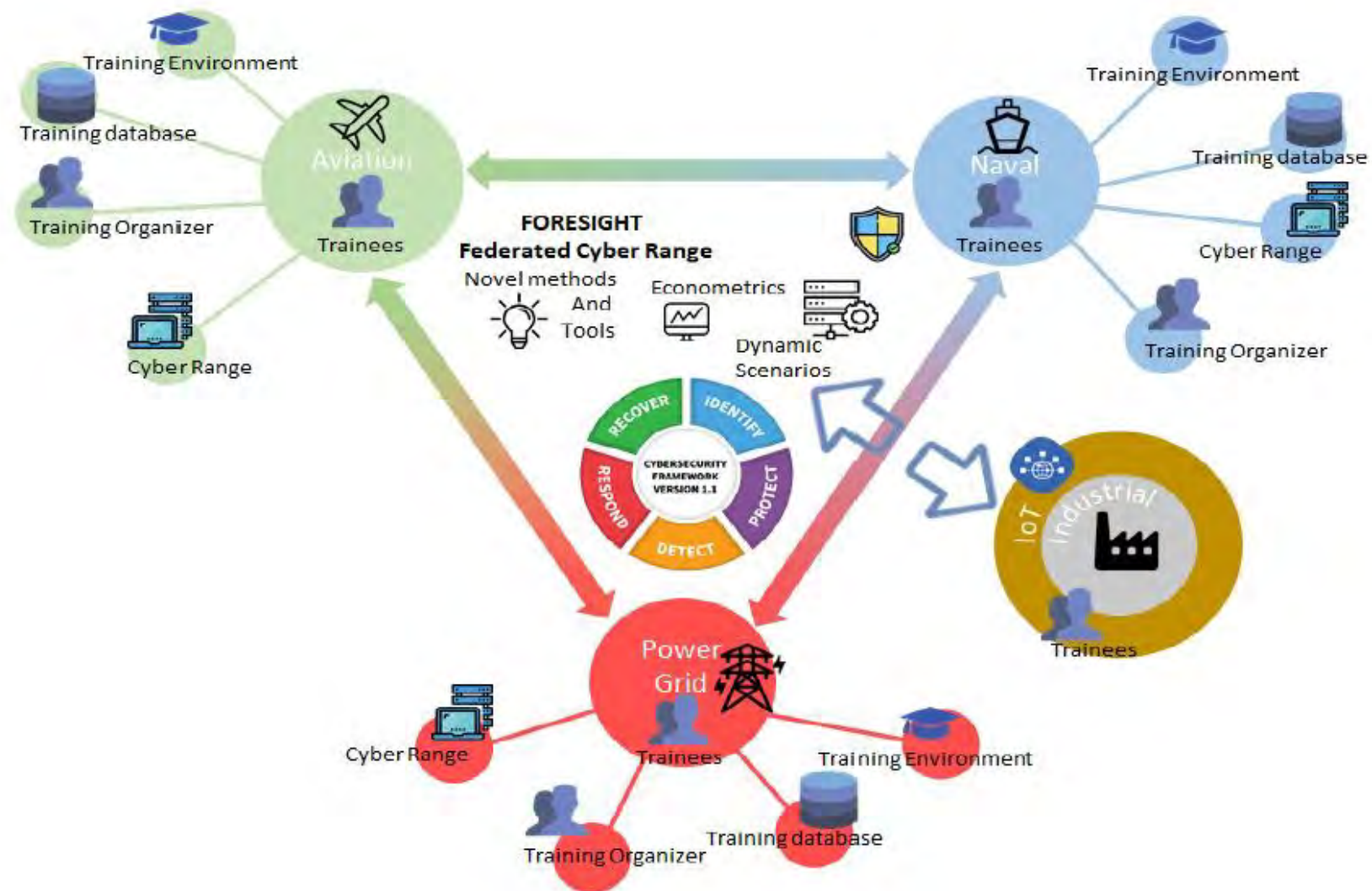
FORESIGHT TEs:

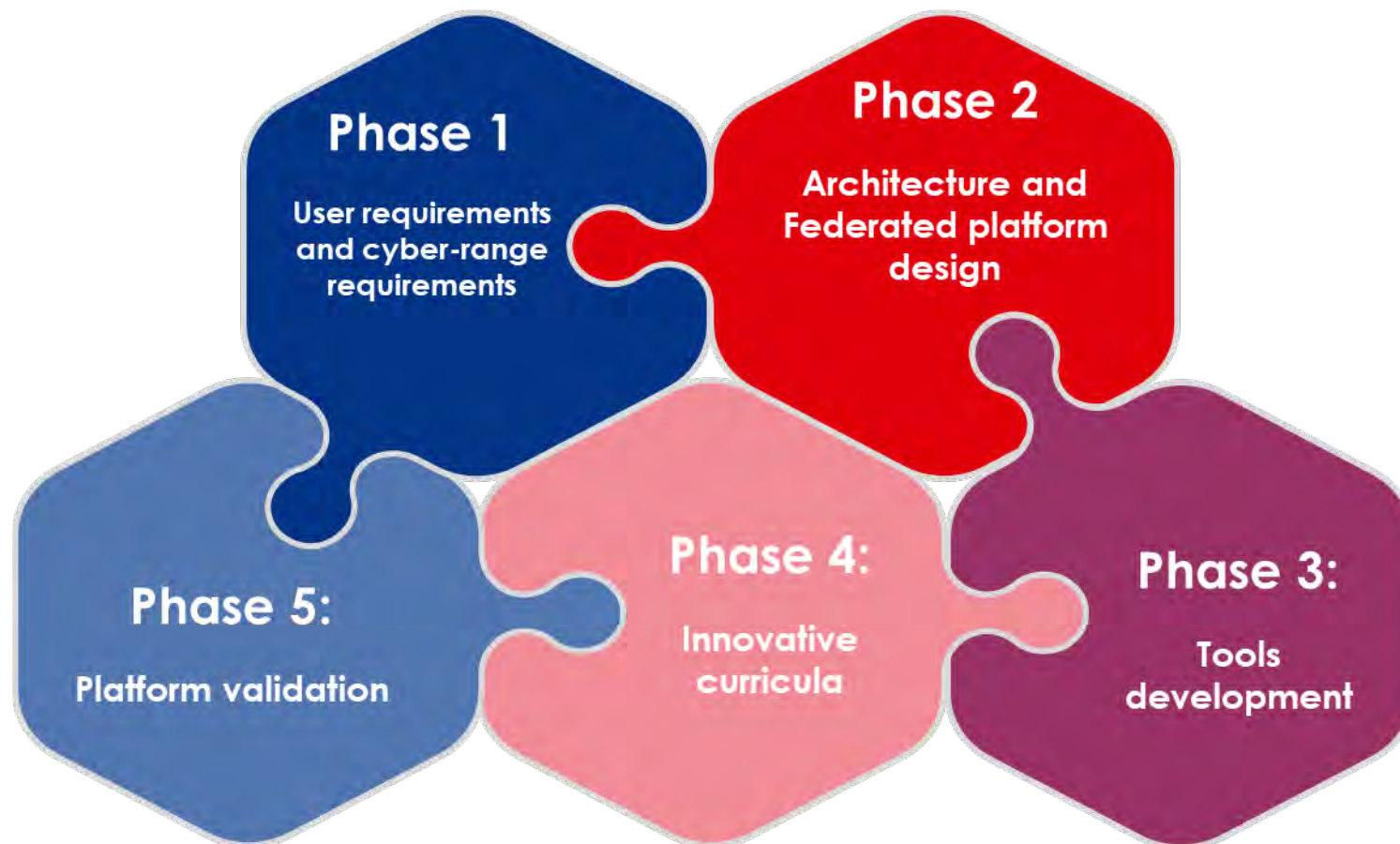
- 6 Technical Experts from 4 different countries.
- Used to train and educate the next generations of cyber security experts in the fields of
 - penetration testing
 - digital forensics
 - malware analysis
 - vulnerability identification
 - patching and incident response

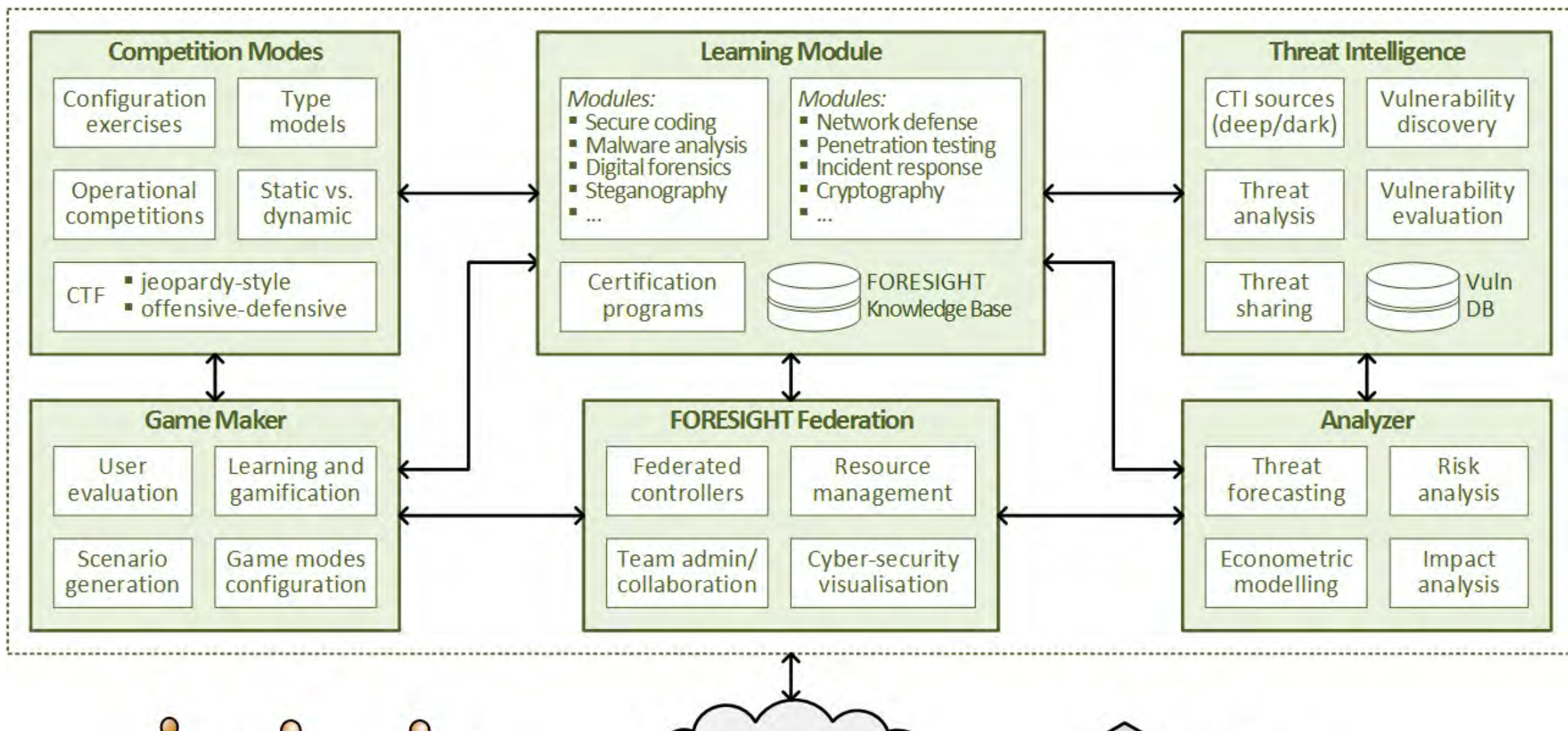


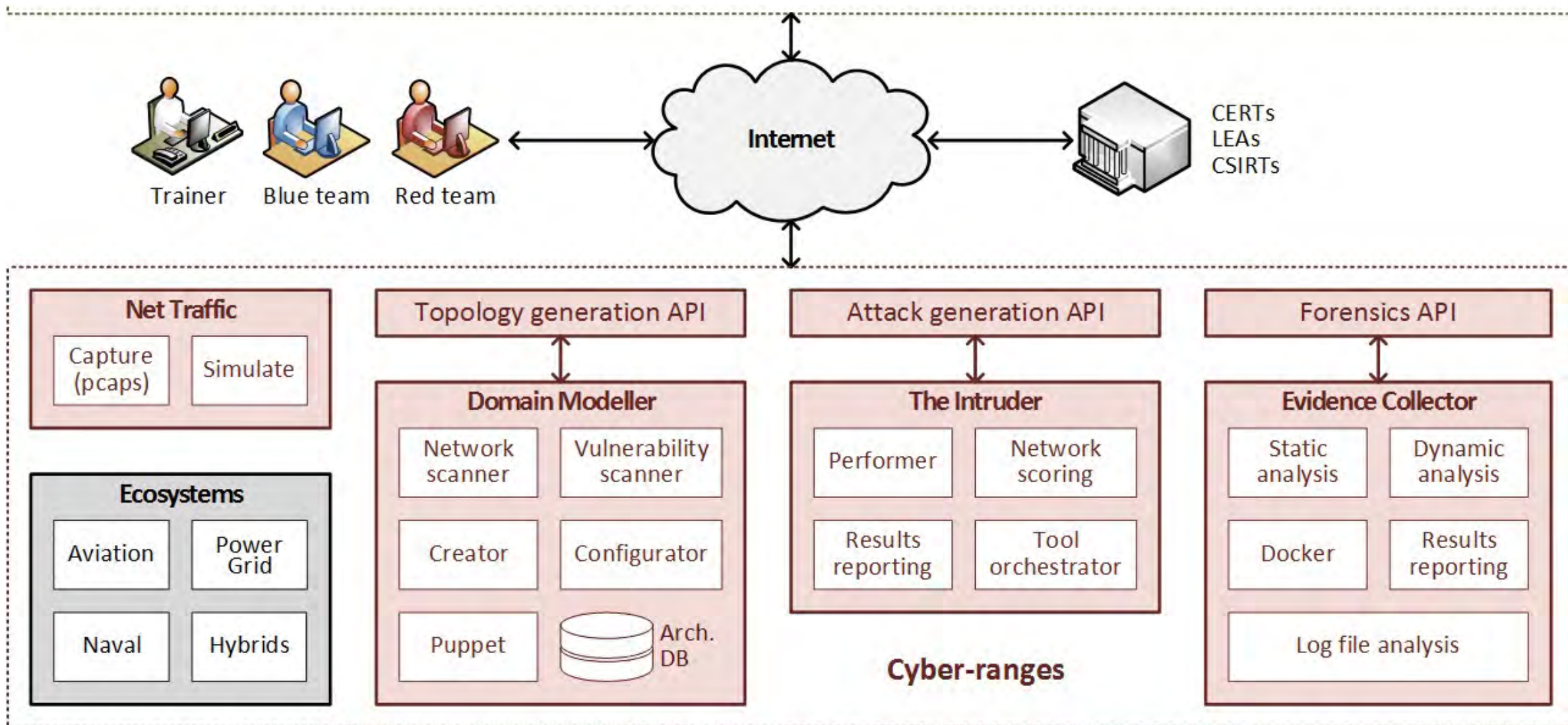
FORESIGHT high-level concept

- Aviation
- Power grid
- Naval
- Hybrid/IoT



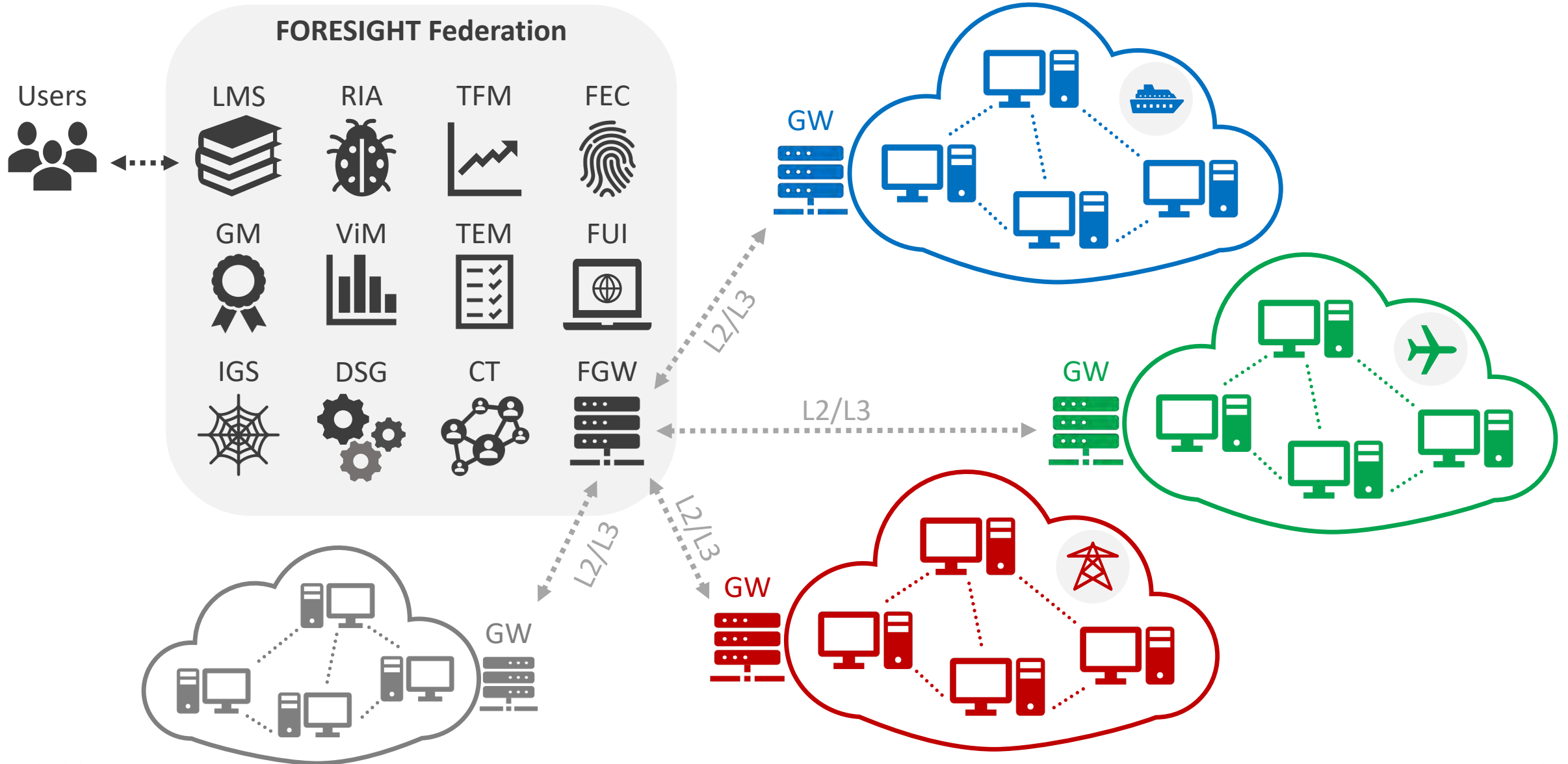






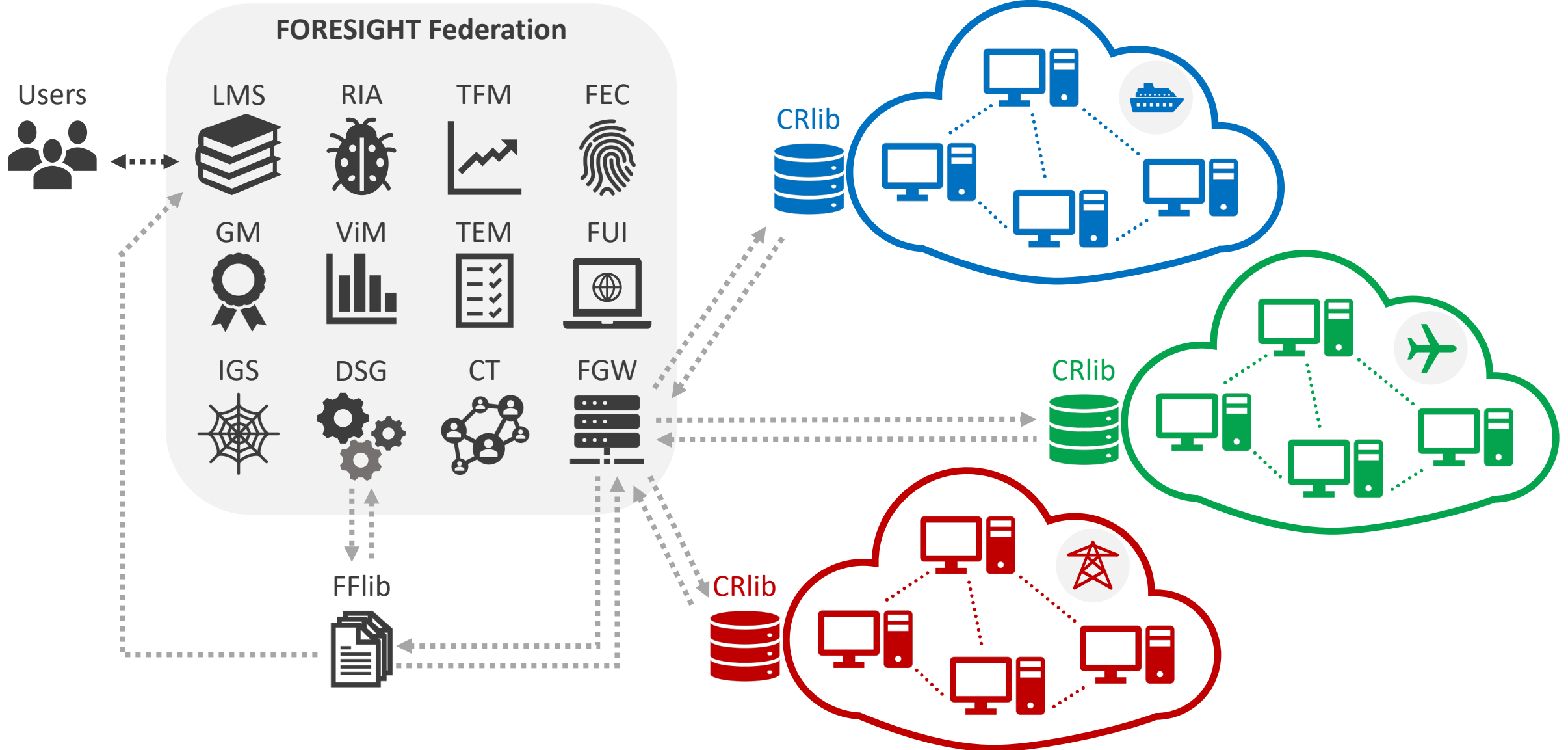
FORESIGHT Federated Platform

... unique features and services



FORESIGHT Federated Platform

Cross-domain and Dynamic Aspects





Individual skills
for standalone
cyber-security
techniques



Team skills
for cooperation and
communication, both within
organization and with external,
collaborating organizations



Skills
to interact with and benefit
from expertise from specialized
security bodies
(CSIRTs)

Varying levels of difficulty
Different training modes
Certification based on standards

Real-world attacks scenarios
Deal with the many facets of cyber-security
Scalable, cost-effective and easy to use Programs

A total of 60 modules are offered and organised by learning paths

- Learning Path 1
Naval (2 courses, 7 modules)
- Learning Path 2
Power Grid (3 courses, 12 modules)
- Learning Path 3
Aviation (3 courses, 7 modules)
- Learning Path 4
General (7 courses, 34 modules)

FORESIGHT Naval Certifications

- Naval
- Power Grid
- Aviation

Classification as

- Cybersecurity Awareness (beginners)
- Intermediate Cybersecurity (intermediate)
- Cybersecurity Professional (advanced)



