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

Cyber Range Network

Joint Webinar

KEMEA-UOP

Dimitrios Kavallieros (Project Coordinator)
Nicholas Kolokotronis (Technical Coordinator)

Cyber Range Network Joint Webinar

26/11/2020

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

General information

H2020-SU-DS-2018 SU-DS01-2018 Innovation Action

Topic SU-DS01-2018 “Cybersecurity preparedness – cyber range, simulation and economics”

DURATION: 10/2019 – 09/2022

GRANT Agreement No. 833673

- 22 partners
- 9 EU member states
- Overall budget ≈ 7,3 m
- Actual budget ≈ 5,9 m

Partners

FORESIGHT

Project Coordinator

KEMEA

Partners

European Dynamics

iti Information Technologies Institute

Cybercrime Research Institute

inCITES Consulting S.A.R.L

CENTRIC Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

MINDS & SPARKS

Abertay University

AIRBUS

OPEN UNIVERSITY OF CYPRUS

ECOLE NAVALE

CYBEXER TECHNOLOGIES

ATHENS INTERNATIONAL AIRPORT

THALES

РАЗПРЕДЕЛЕНИЕ

CERT.BG COMPUTER EMERGENCY RESPONSE TEAM BULGARIA

ieit

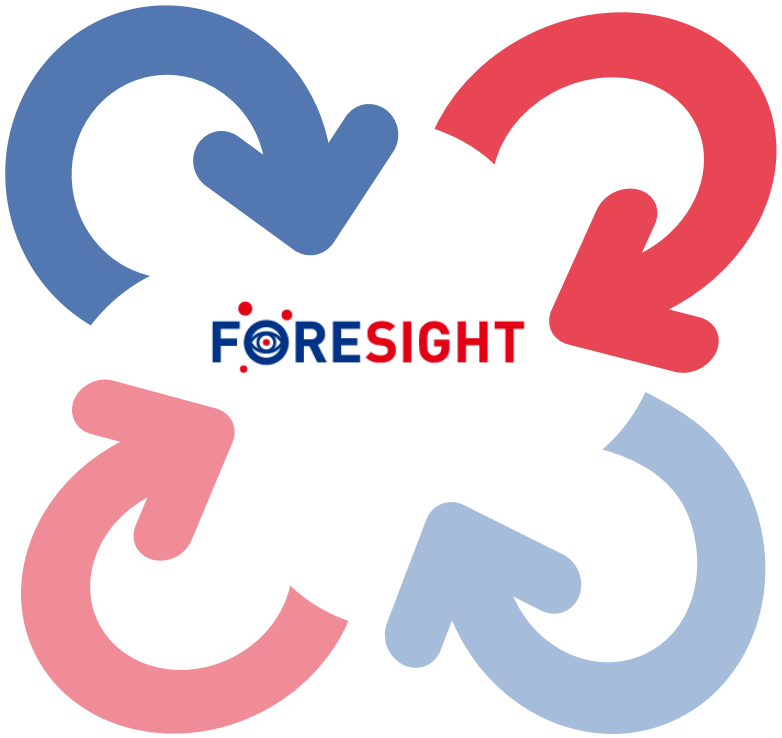
ESO

University of Strathclyde Glasgow

UNIVERSITY OF PORTSMOUTH

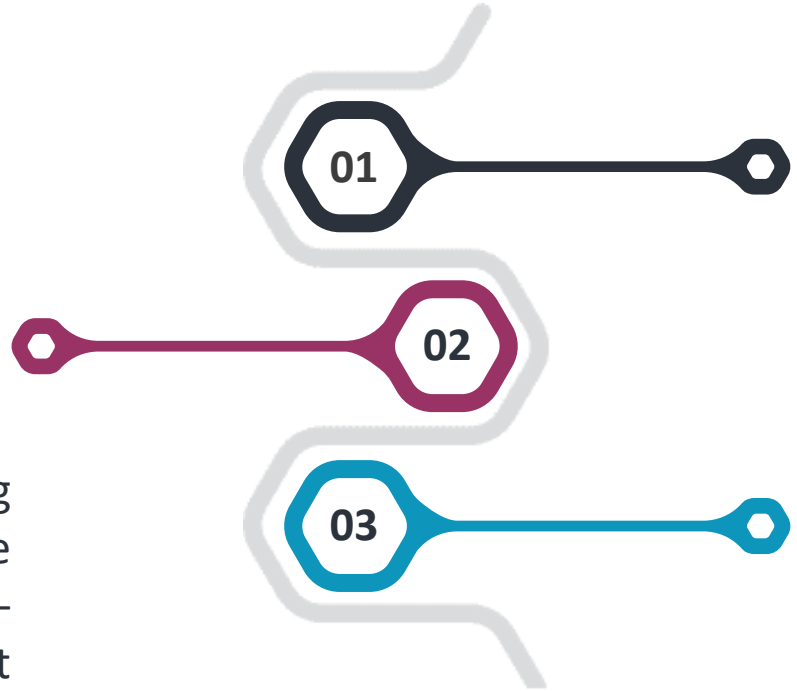
FORESIGHT motivation

- ✓ 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

FORESIGHT scope



Federated cyber range

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

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

ecosystem of networked realistic training and simulation platforms

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

FORESIGHT Objectives

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).

CR Federation Concept

As defined in ECSO WG5 paper (Mar. ‘20)

A federated CR solution that

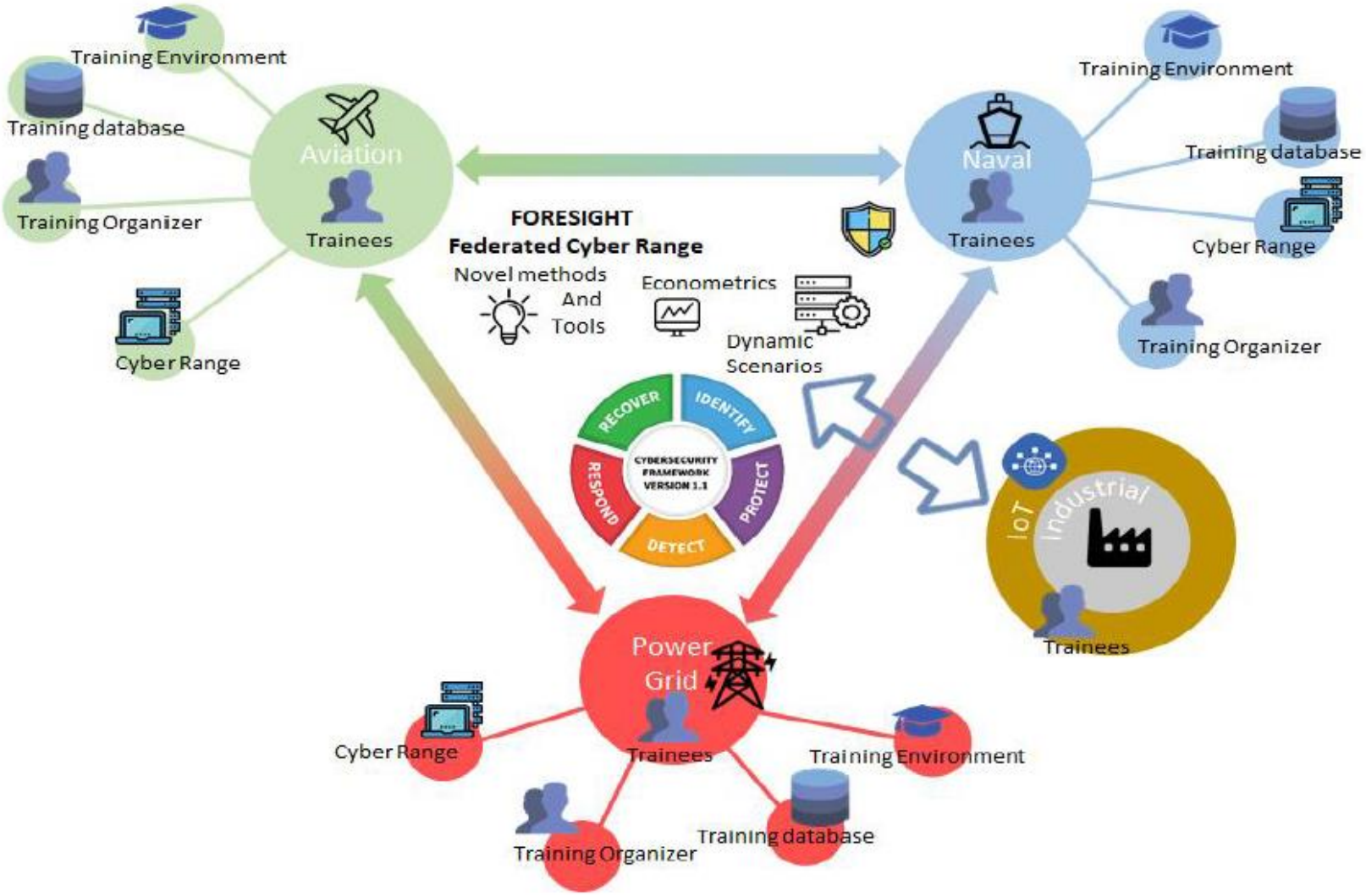
- agrees upon standards of operation (scenario/capabilities description language) in a collective fashion
  - can request provisioning of CR services within the federation
  - each CR to implements/delivers them in own specific way
- complex and costly capabilities and functionalities are shared to achieve multiple UCs

Typically, can also encompass the *integration concept*, in which peer CRs

- communicate with each other to deliver a scenario / simulation ENV spread across them
- plan the integrated network environment (IP address spaces, etc.)

FORESIGHT high-level concept

- Aviation
- Power grid
- Naval
- Hybrid/IoT



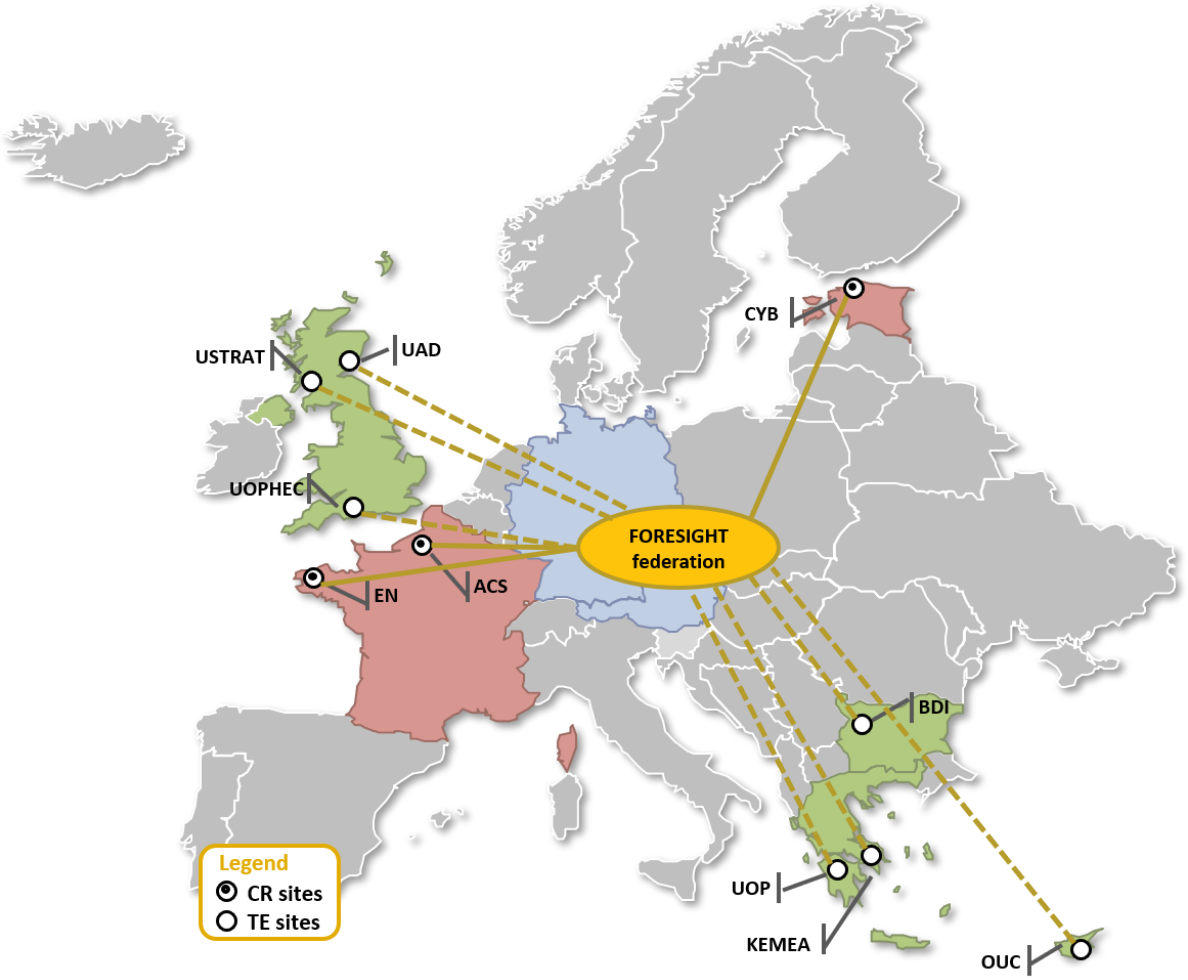
FORESIGHT federation platform for CRs/TEs

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

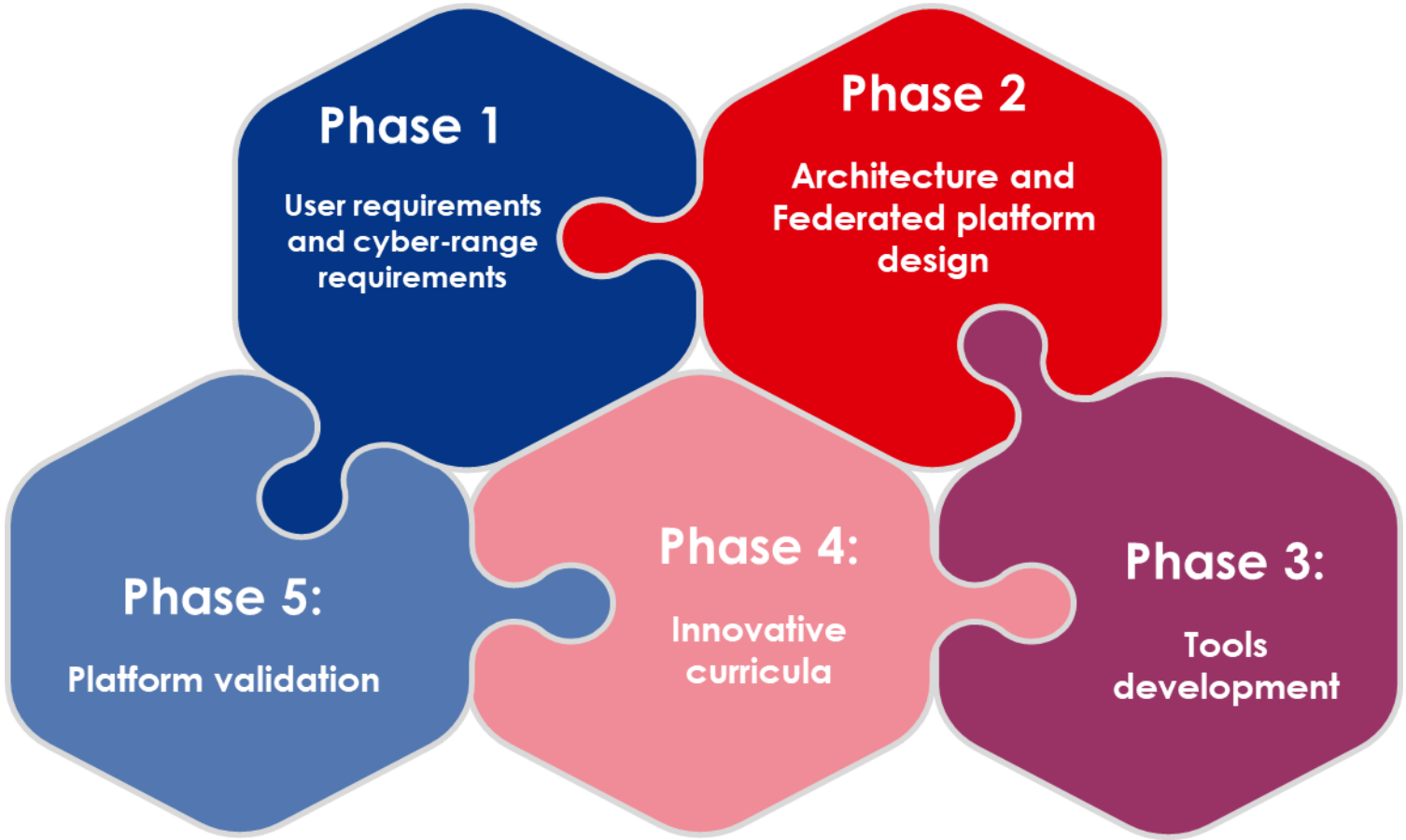


FORESIGHT Federation Approach

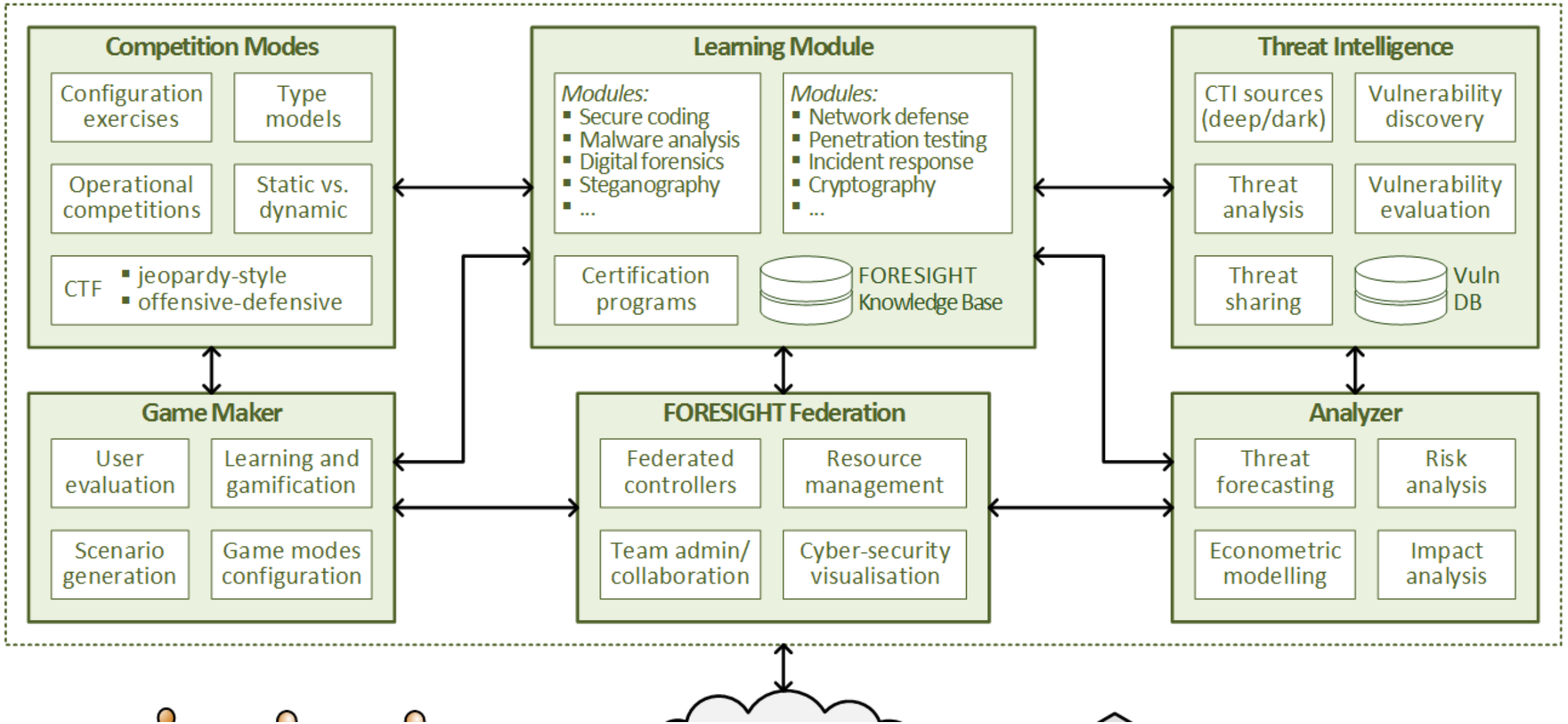
A federated CR solution that

- brings together unique cyber-security aspects from each domain
- considerably extends the capabilities of existing CRs by … allowing complex cross-domain (i.e. hybrid) scenarios to be built
  - … interactions with the much wider IoT ecosystem
- meets the most demanding REQs in terms of ecosystem modelling complexity and training needs
- caters for multi-domain training requirements by allowing CRs to connect to each other
- makes available to users a wider range of educational services and material, allowing them to obtain training regarding a broader spectrum of cyber-attacks
- advances the skills of cyber-security professionals … while providing a series of unique features and services (like threat forecasting, risk evaluation, econometric models, etc.)

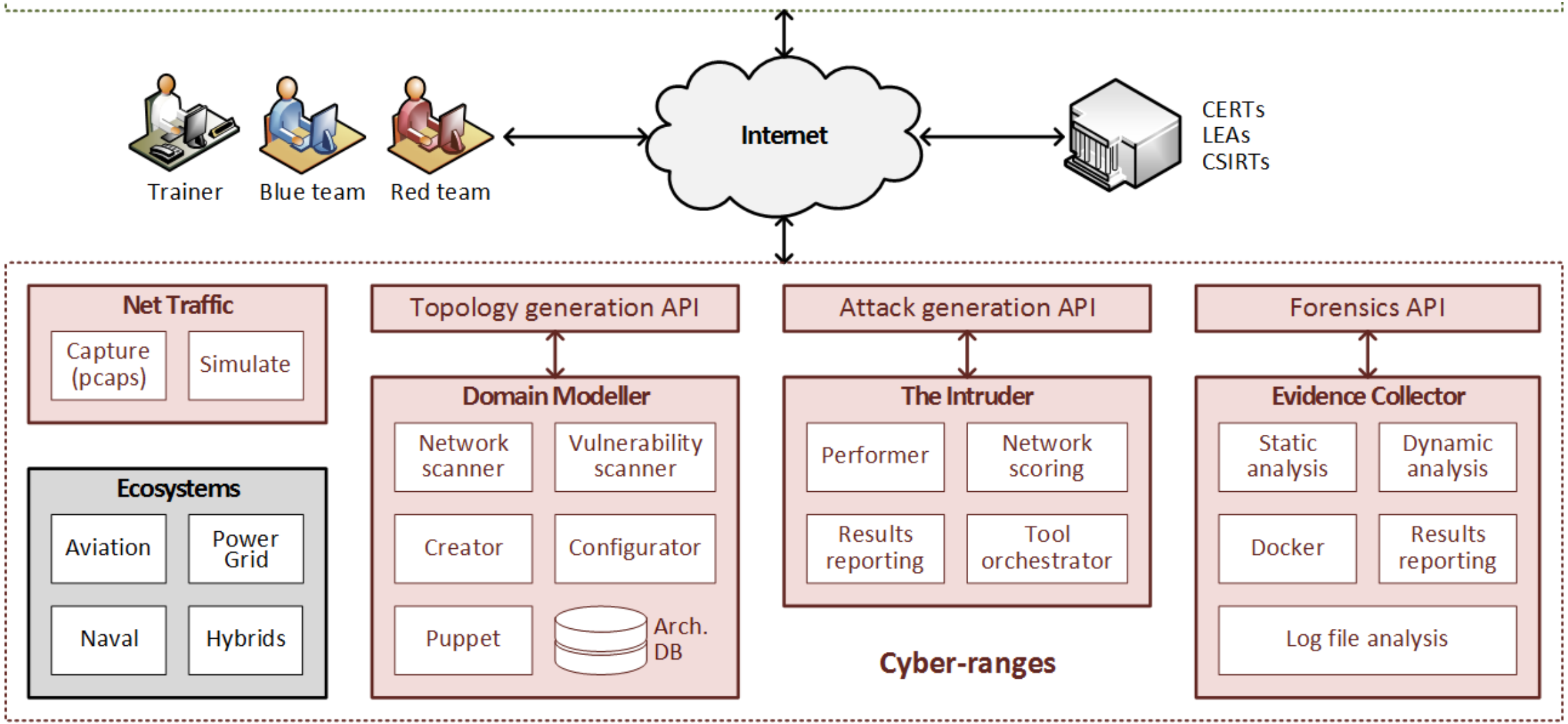
FORESIGHT methodology



FORESIGHT high-level architecture

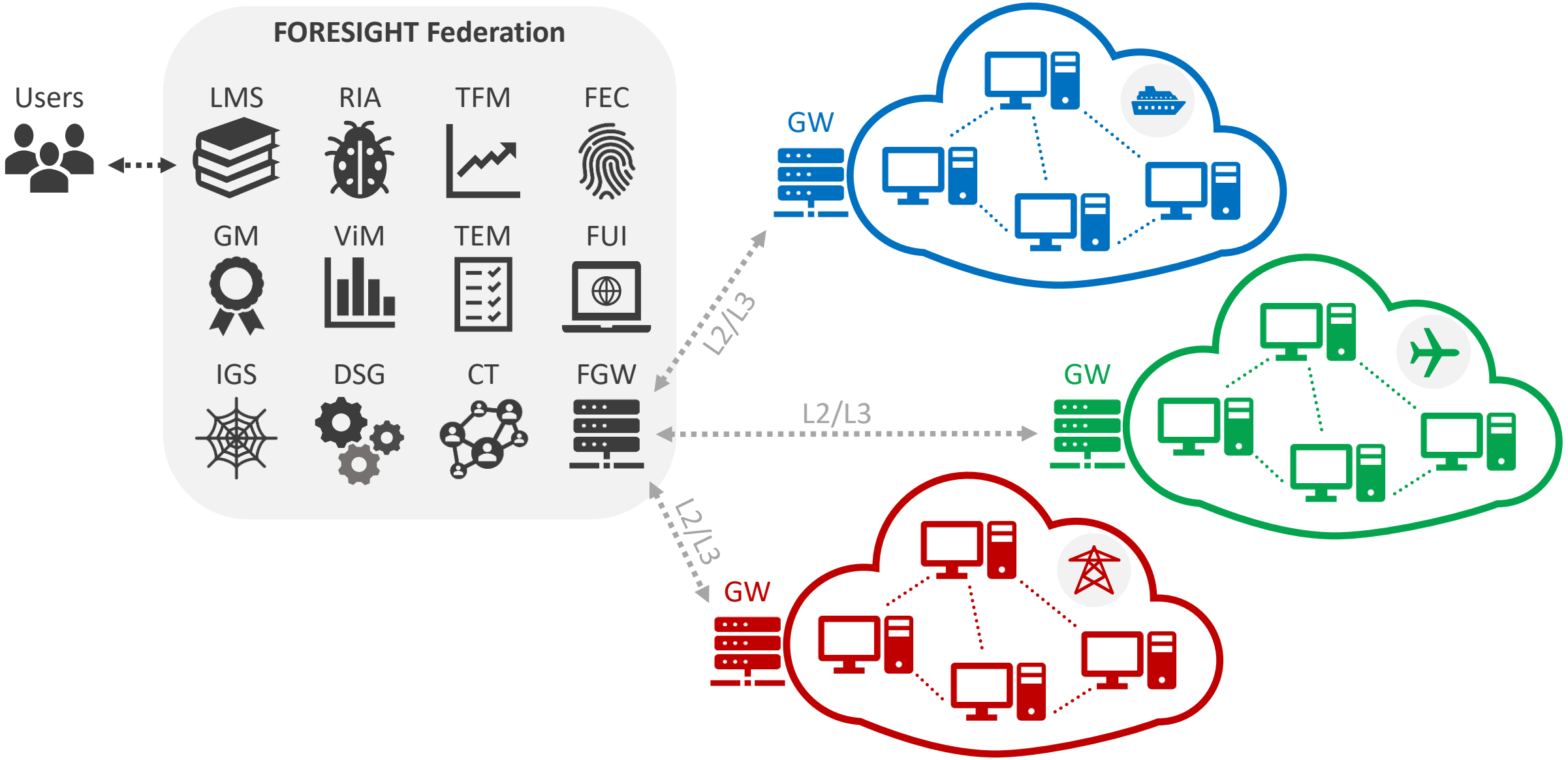


FORESIGHT high-level architecture



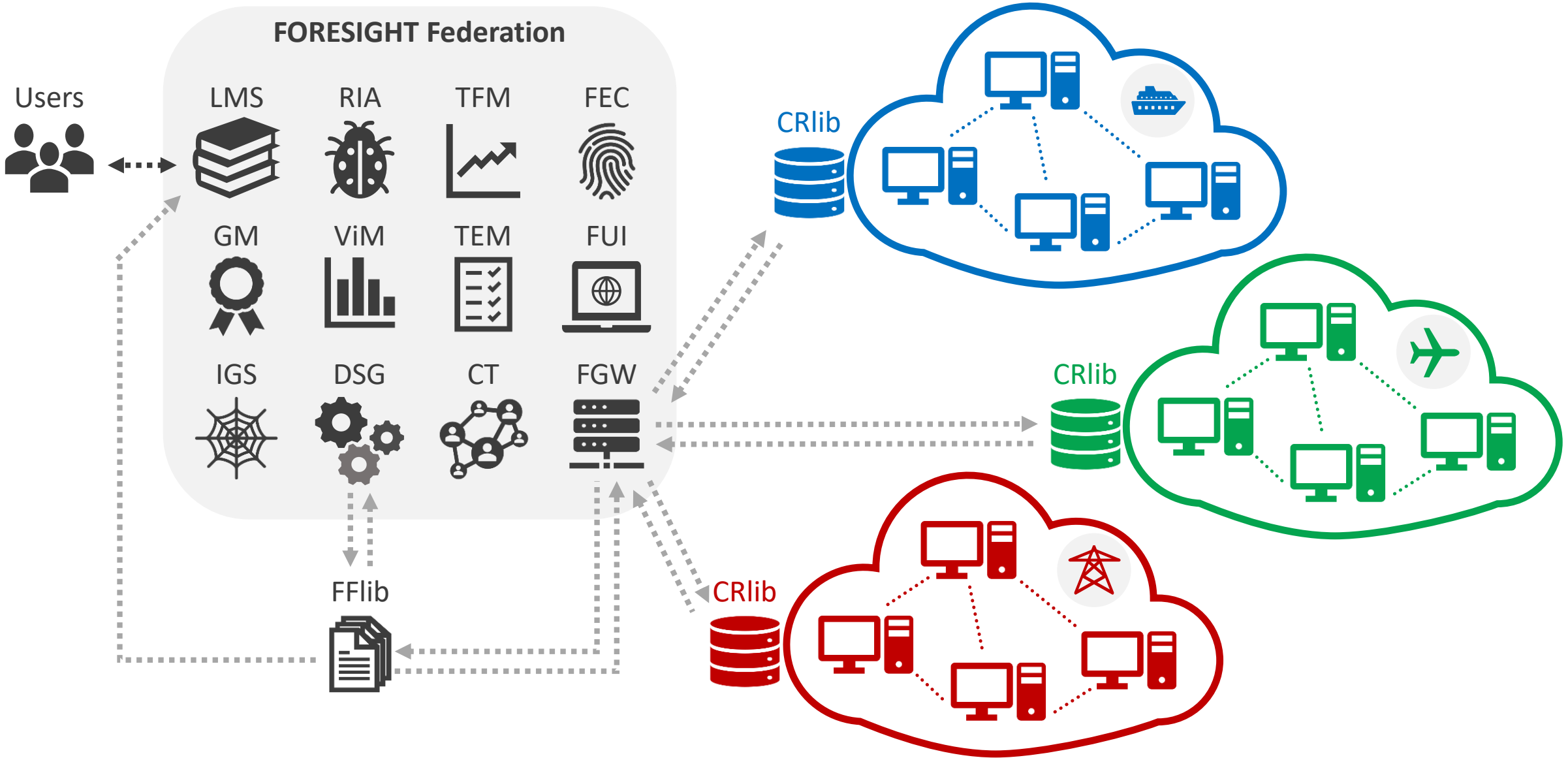
FORESIGHT Federated Platform

… unique features and services



FORESIGHT Federated Platform

Cross-domain **and Dynamic** Aspects

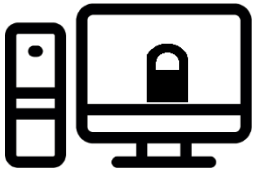


FORESIGHT Training and Certification

Main pillars

Individual skills
for standalone
cyber-security
techniques

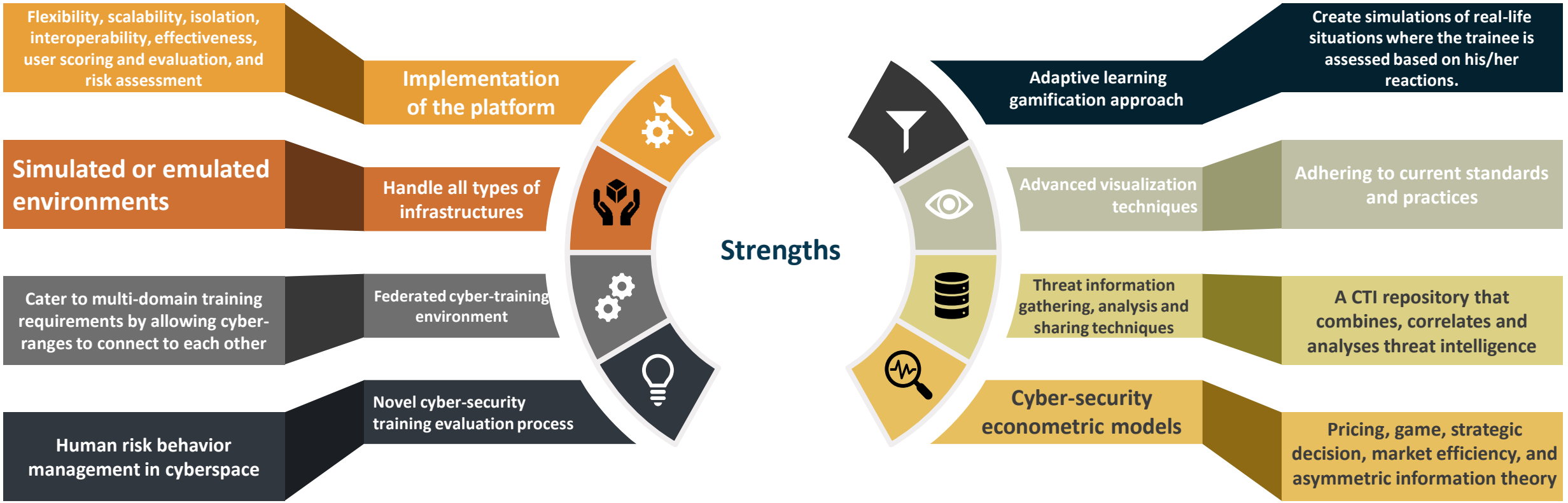
Team skills
for cooperation and
communication, both within
organization and with external,
collaborating organizations



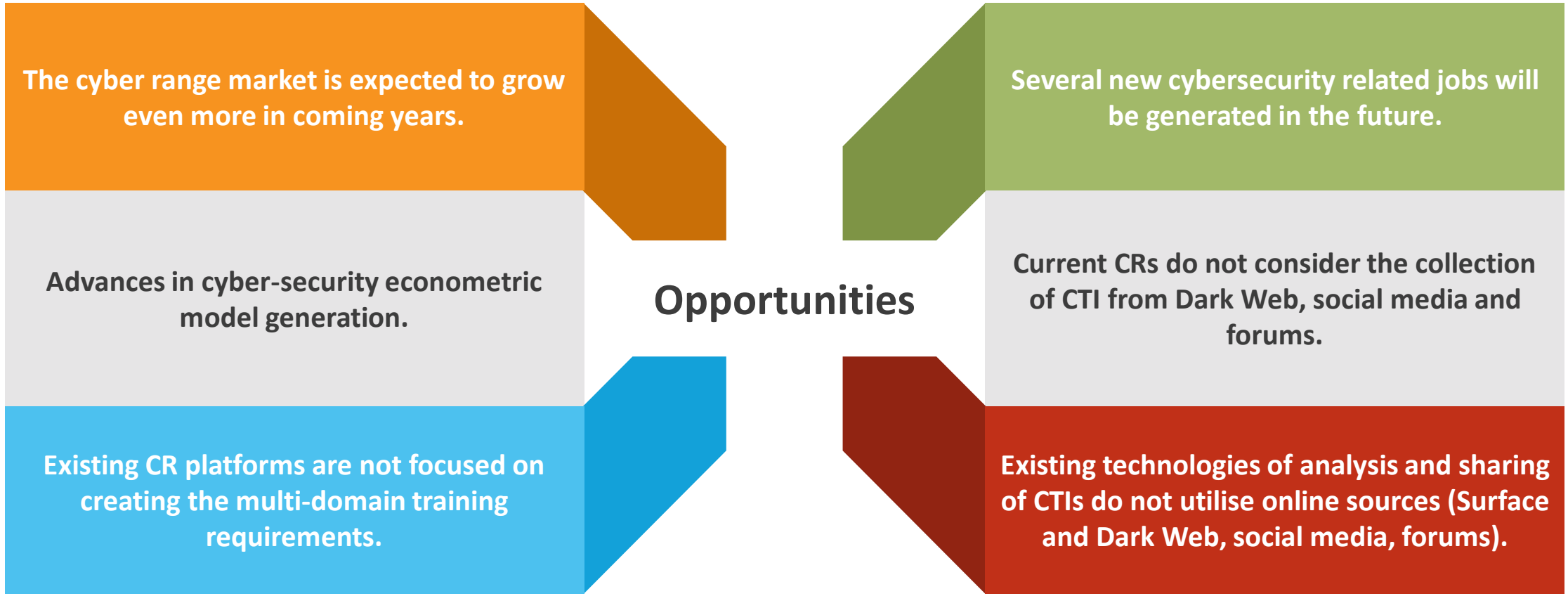
Skills
to interact with and benefit
from expertise from specialized
security bodies
(CSIRTs)

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

FORESIGHT Innovation potential (1/2)



FORESIGHT Innovation potential (2/2)




THANK
YOU
GRAZIE
MULTUMESC
MERCI
MAAKE
TERMA KASIH
RAIBH MAITH AGAT
JUSPAXAR
OBRIGADO
MATONDO
KIITOS
SALAMAT
MOCHCHAKKERAM
KIA ORA
MULTUMESC
CHOKRANE
SALAMAT
CAM ON BAN
MERCI
RAIBH MAITH AGAT
OBRIGADO
MOCHCHAKKERAM
ASANTE
UA TSAUG RAU KOJ
MOCHCHAKKERAM
KIITOS
VINAKA
OBRIGADO
DANK JE
NIRRINGRAZZJAK
MAMANA
MULTUMESC
KIITOS
DANKON
NIRRINGRAZZJAK
MOCHCHAKKERAM
ARIGATO
MOCHCHAKKERAM
OBRIGADO
SPASIBO
WELALIN
SPASIBO
MAAKE
OBRIGADO
SPASIBO
RAIBH MAITH AGAT
DANK JE
MATONDO
CHOKRANE
UA TSAUG RAU KOJ
CHOKRANE
MATUR NUWUN
MERCI
MOCHCHAKKERAM