FORESIGHT project: Development of a federated cyber range platform and innovative training curricula

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

Training the European workforce of tomorrow: cyber ranges in practice | Webinar

17/05/2022

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

Partners

FORESIGHT

Project Coordinator

KEMEA

10.2019 – 03.2023

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

Project 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 ELEFTHERIOS VENIZELOS

THALES

РАЗПРЕДЕЛЕНИЕ

CERT.BG COMPUTER EMERGENCY RESPONSE TEAM BULGARIA

ИНСТИТУТ ПО ОТБРАНА

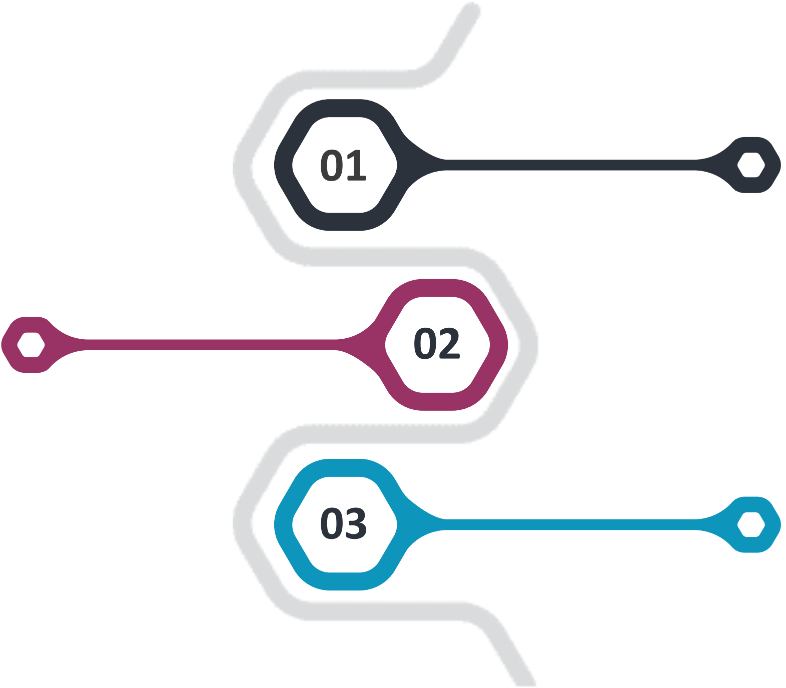
ieit

ESO

University of Strathclyde Glasgow

UNIVERSITY OF PORTSMOUTH

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 allow creating complex cross-domain scenarios jointly with the IoT domain

ecosystem of networked 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

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.)

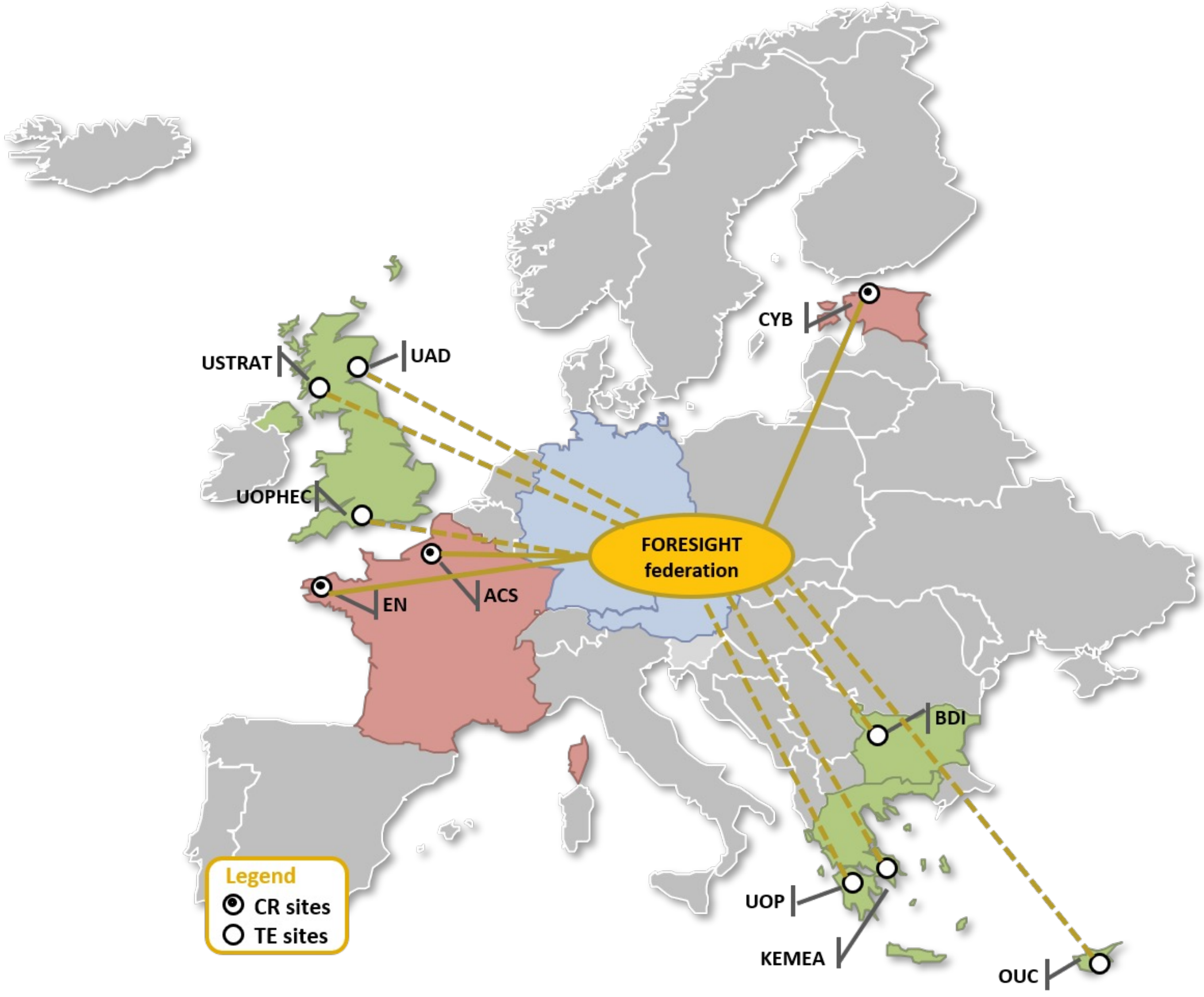
FORESIGHT federation platform for CRs/TEs

FORESIGHT CRs

- 3 different cyber-ranges from two countries
  - **CybExer** (EE)
  - **Airbus** and **Naval Academy** (FR)
- Developed for different domains
- Provide professional training on preparedness and incident response to cyber security experts

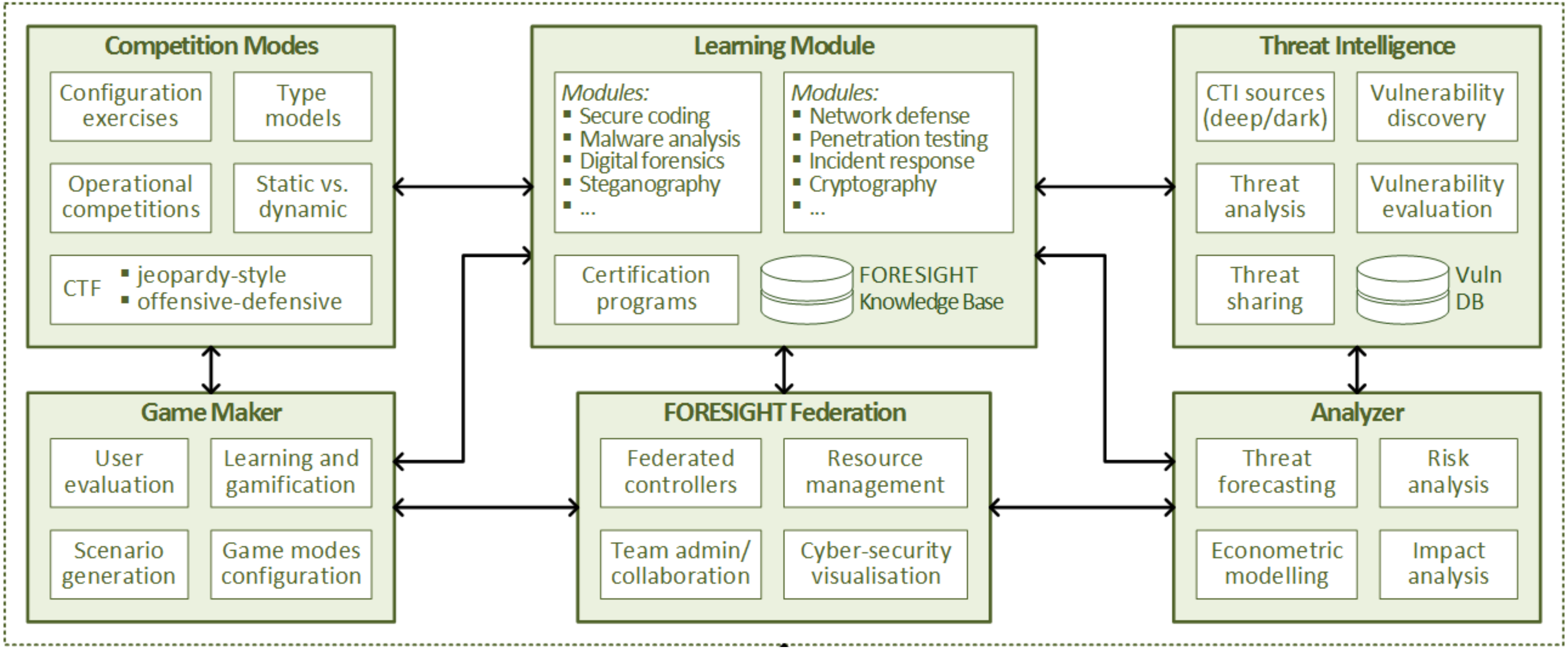
FORESIGHT TEs

- 6 training environments from four countries
  - **KEMEA, UOP** (GR) and **OUC** (CY)
  - **BDI** (BG) and **UOPHEC, USTRAT** (UK)
- Mainly used for security education in the fields of
  - penetration testing
  - digital forensics
  - malware analysis
  - vulnerability assessment
  - incident response



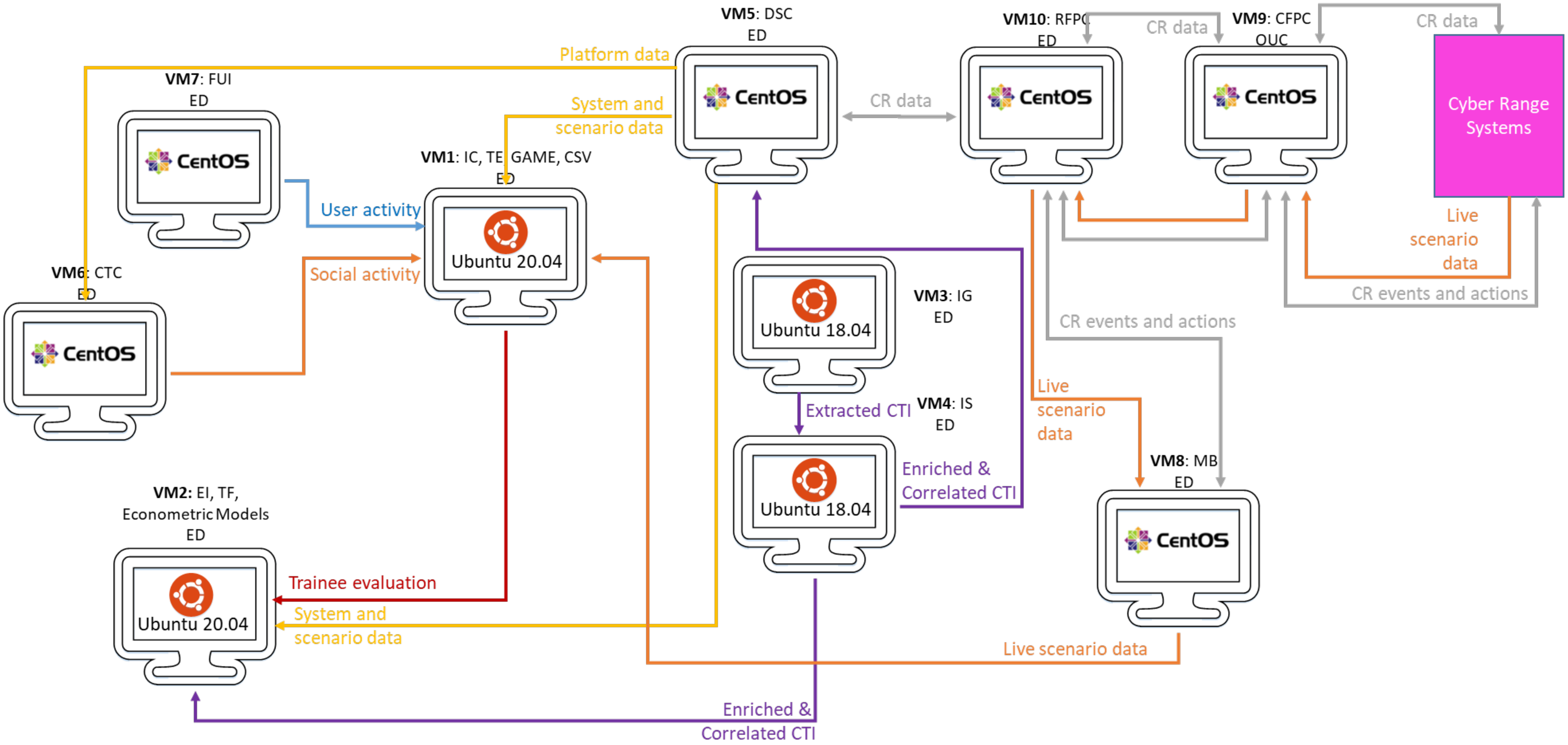
FORESIGHT high-level architecture

Component view



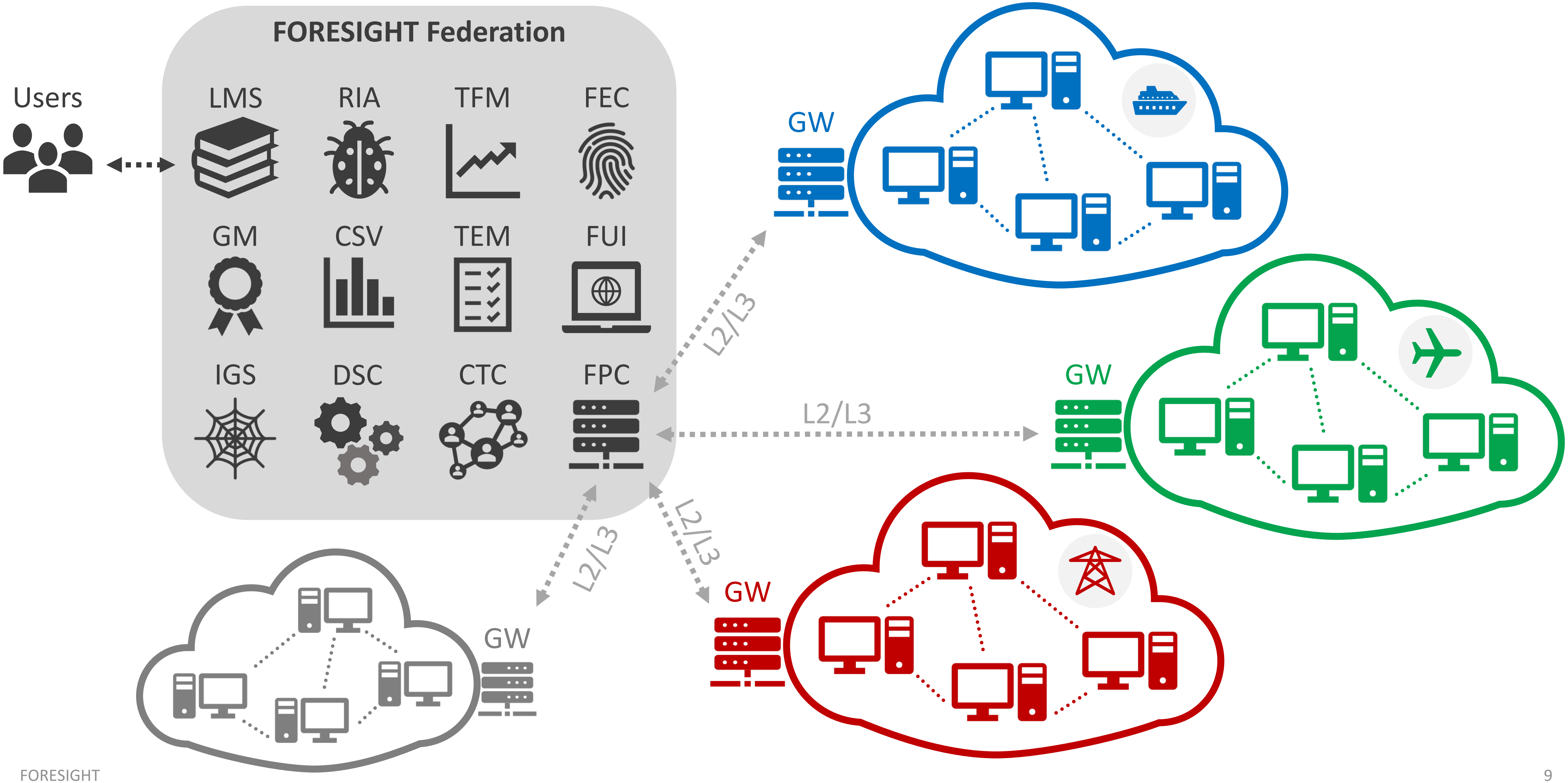
FORESIGHT high-level architecture

Deployment view

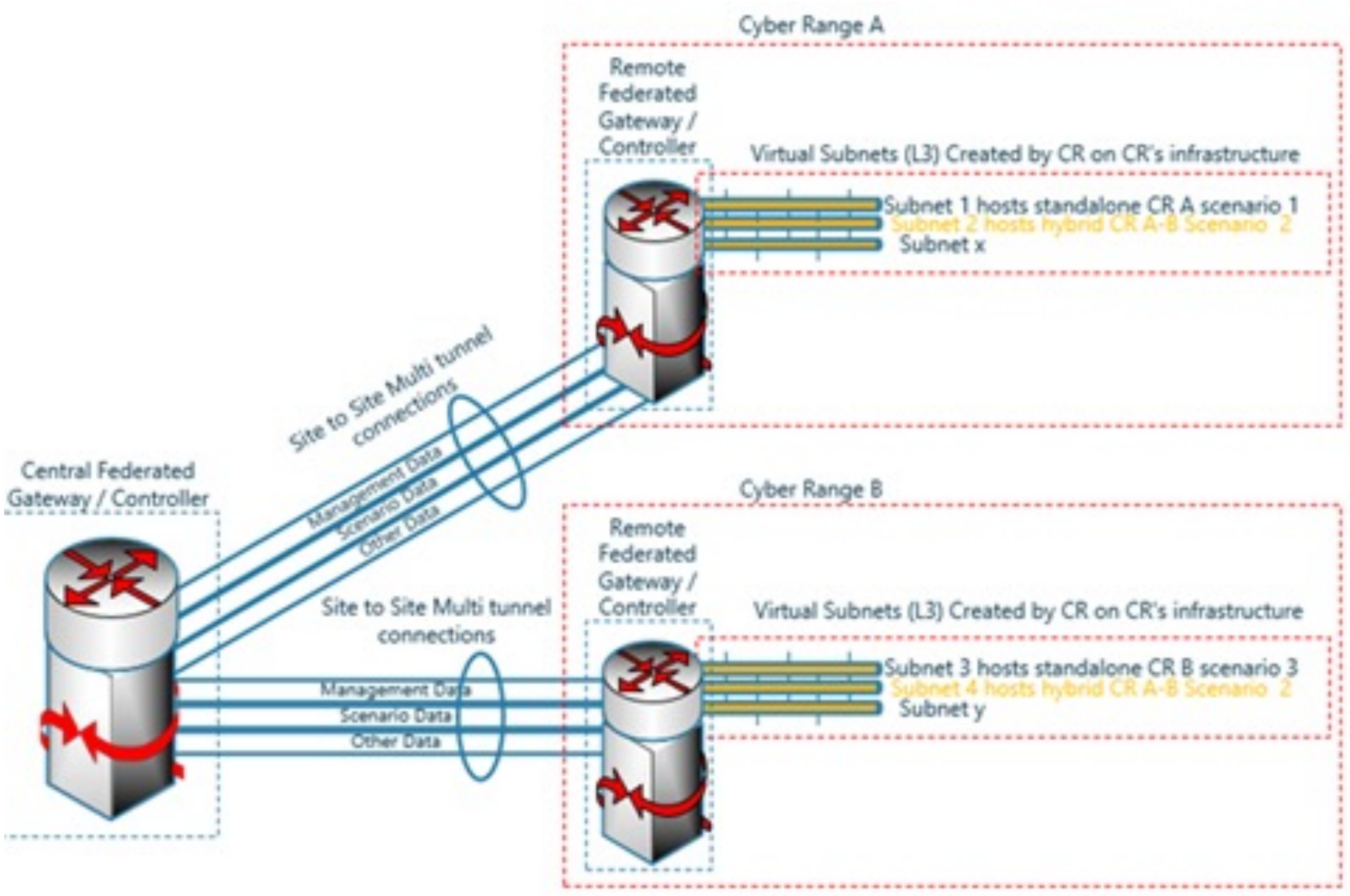


FORESIGHT Federated Platform

… unique features and services



FORESIGHT high-level architecture



Cyber Range A
Remote Federated Gateway / Controller
Virtual Subnets (L3) Created by CR on CR's infrastructure
Subnet 1 hosts standalone CR A scenario 1
Subnet 2 hosts hybrid CR A-B Scenario 2
Subnet x
Site to Site Multi tunnel connections
Management Data
Scenario Data
Other Data
Central Federated Gateway / Controller
Cyber Range B
Remote Federated Gateway / Controller
Virtual Subnets (L3) Created by CR on CR's infrastructure
Site to Site Multi tunnel connections
Subnet 3 hosts standalone CR B scenario 3
Subnet 4 hosts hybrid CR A-B Scenario 2
Subnet y
Management Data
Scenario Data
Other Data

U1
- Trainees / defenders (blue team)

U2
- Cyber-attackers (red team)

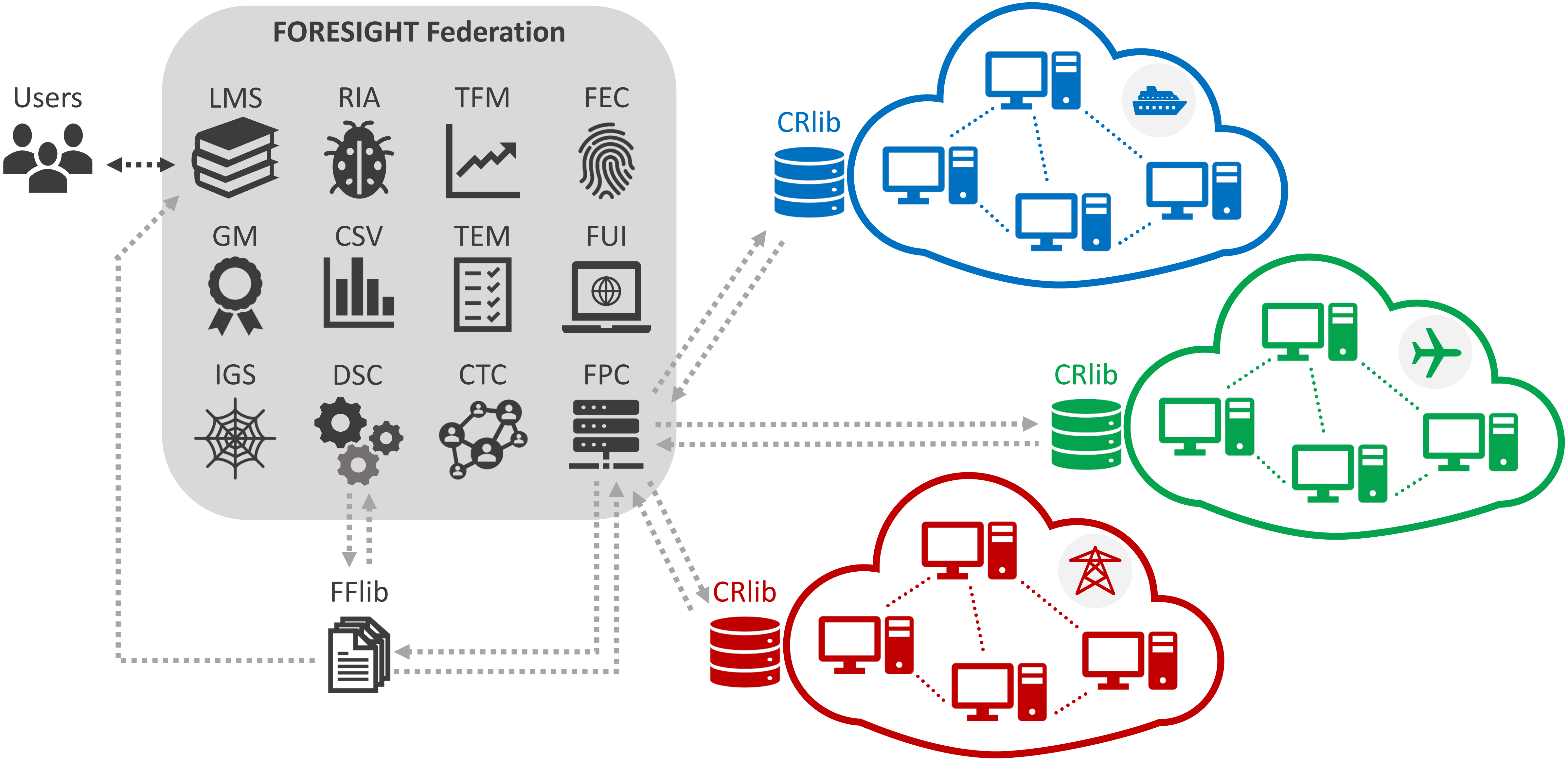
U3
- Training planners

U4
- Federated platform administrators

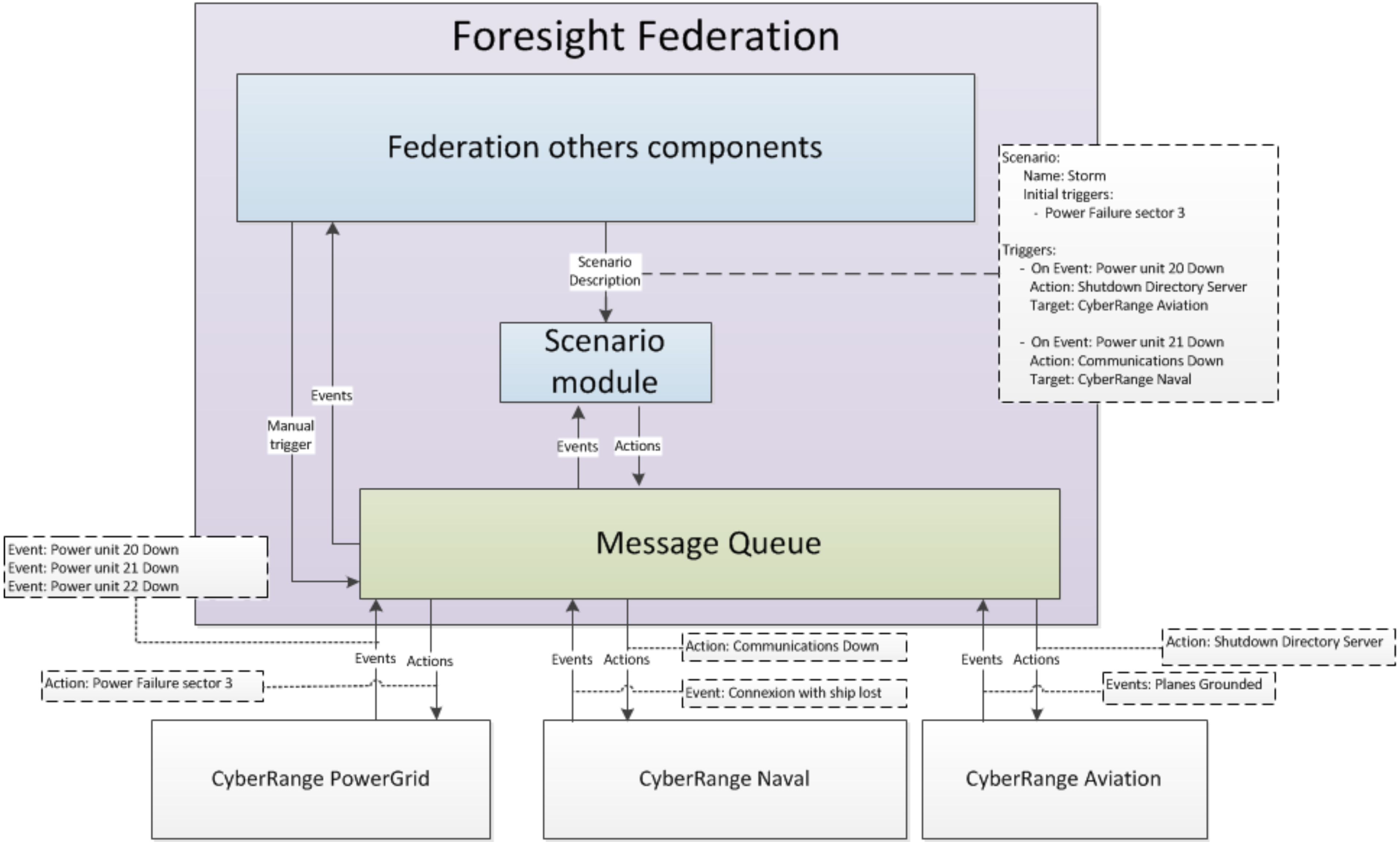
U5
- Peer CR/TE platform admins (federation)

FORESIGHT Federated Platform

Cross-domain **and Dynamic** Aspects



CR information exchange



Scenario:
    Name: Storm
    Initial triggers:
        - Power Failure sector 3

Triggers:
  - On Event: Power unit 20 Down
    Action: Shutdown Directory Server
    Target: CyberRange Aviation

  - On Event: Power unit 21 Down
    Action: Communications Down
    Target: CyberRange Naval

Event: Power unit 20 Down
Event: Power unit 21 Down
Event: Power unit 22 Down

Action: Power Failure sector 3

Action: Communications Down

Event: Connexion with ship lost

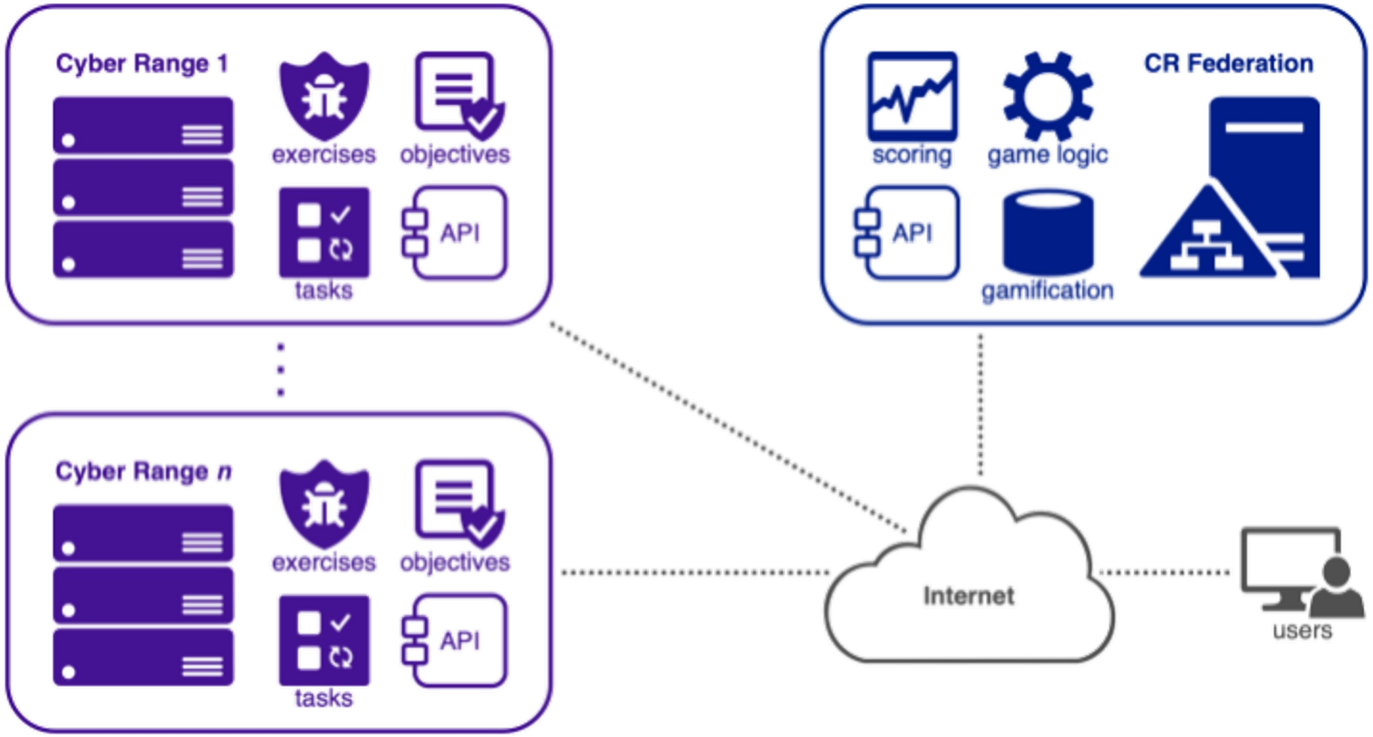
Action: Shutdown Directory Server

Events: Planes Grounded

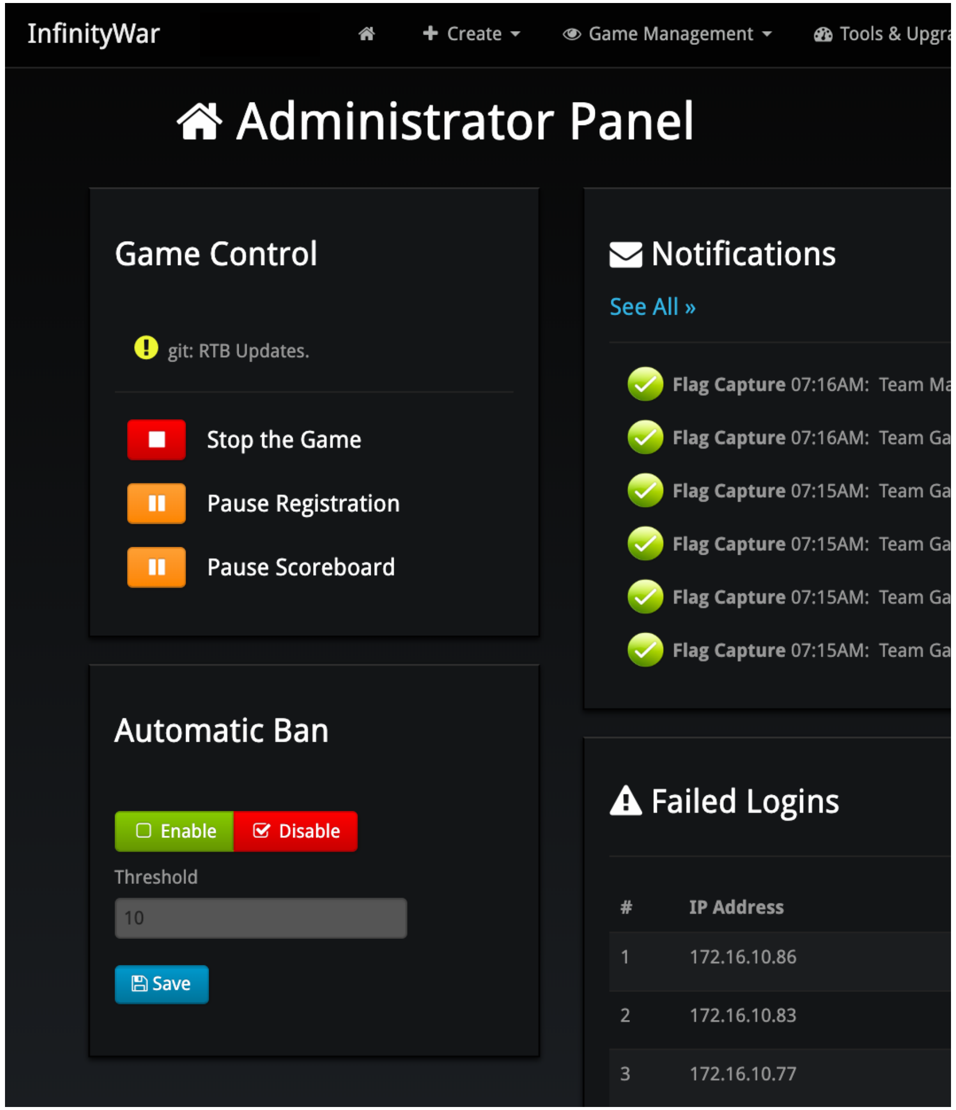
Gamification Scoring Model

Architecture Overview

- Consists of
  - Score calculation mechanism
  - Application programming interfaces
  - Various game mechanisms
- Workflow
  - Exercises’ results retrieved
  - Results are aggregated
  - Scoring / awards are calculated
- Automated trainee evaluation
  - CR-specific tools
  - Scenario-driven



FORESIGHT (Lightweight) Training Environments



Administrator Panel

Game Control

git: RTB Updates.

Automatic Ban

Threshold: 10

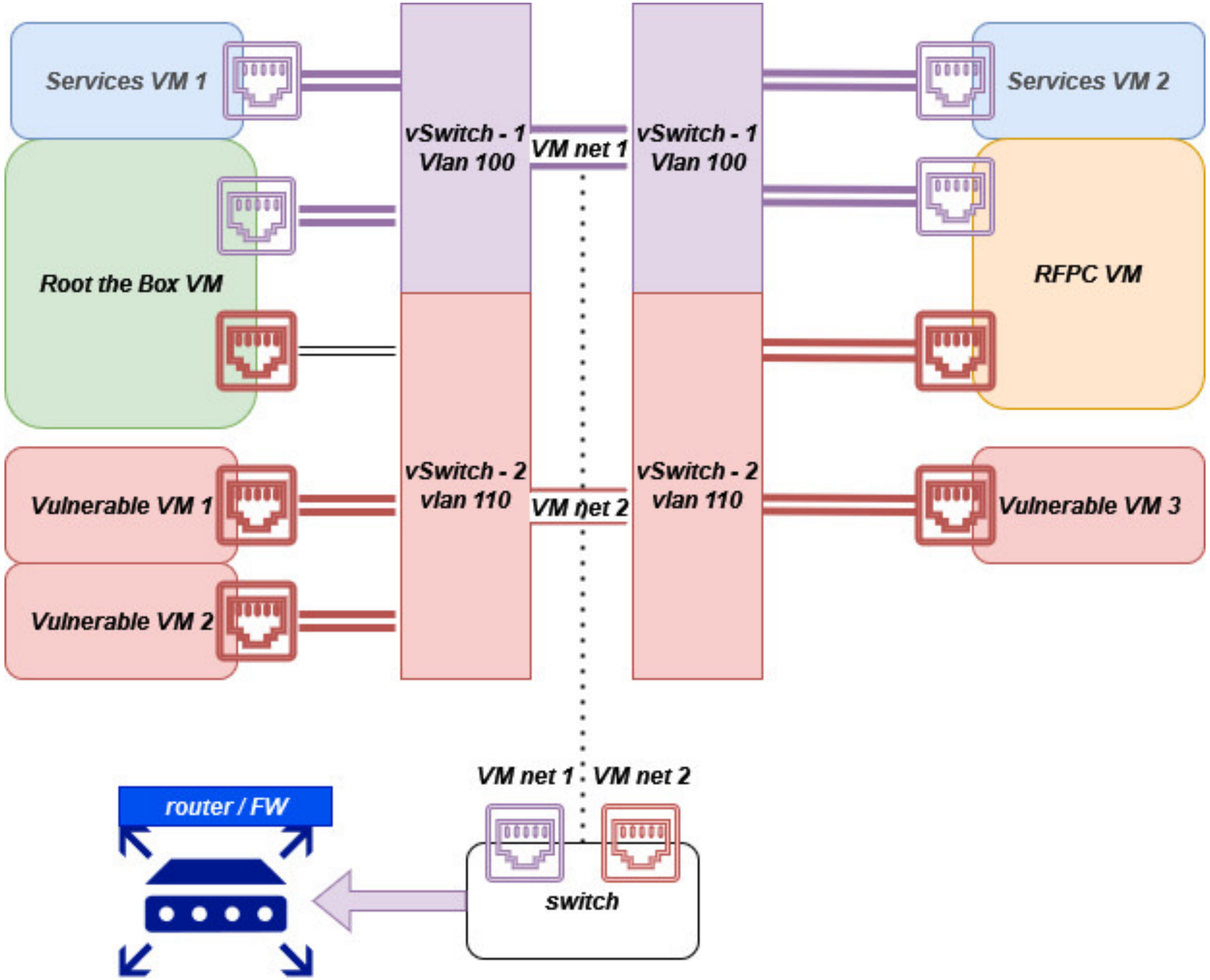
Notifications

See All »

- Flag Capture 07:16AM: Team Ma
- Flag Capture 07:16AM: Team Ga
- Flag Capture 07:15AM: Team Ga
- Flag Capture 07:15AM: Team Ga
- Flag Capture 07:15AM: Team Ga
- Flag Capture 07:15AM: Team Ga

Failed Logins

#	IP Address
1	172.16.10.86
2	172.16.10.83
3	172.16.10.77



FORESIGHT Training and Certification

Main pillars

Individual skills for cyber-security techniques

Team skills for cooperation and communication (within org and externally)

Other skills to interact with/ benefit from the expertise of specialized security bodies

– Different training models
– Varying difficulty levels
– Real-world attack scenarios

– Multi-faceted approach to cyber-security
– Certification based on standards
– Scalable, cost-effective, easy to use programs

FORESIGHT Training and Certification

Learning paths and certifications

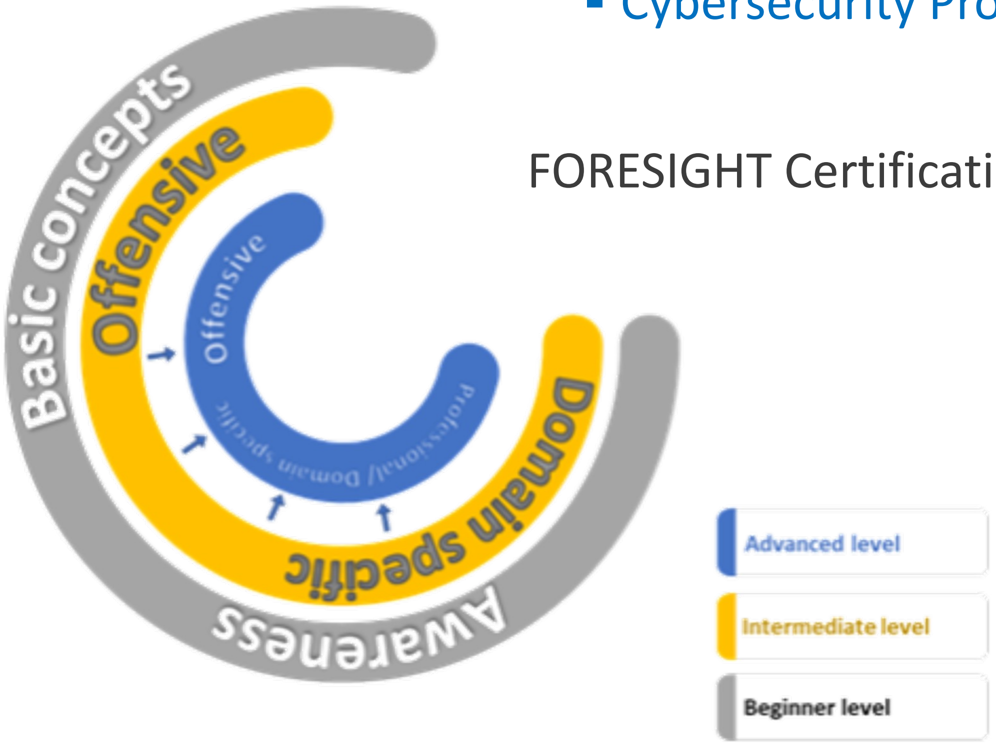
A total of 60 modules are offered and organised by learning paths

- 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)

Classification as

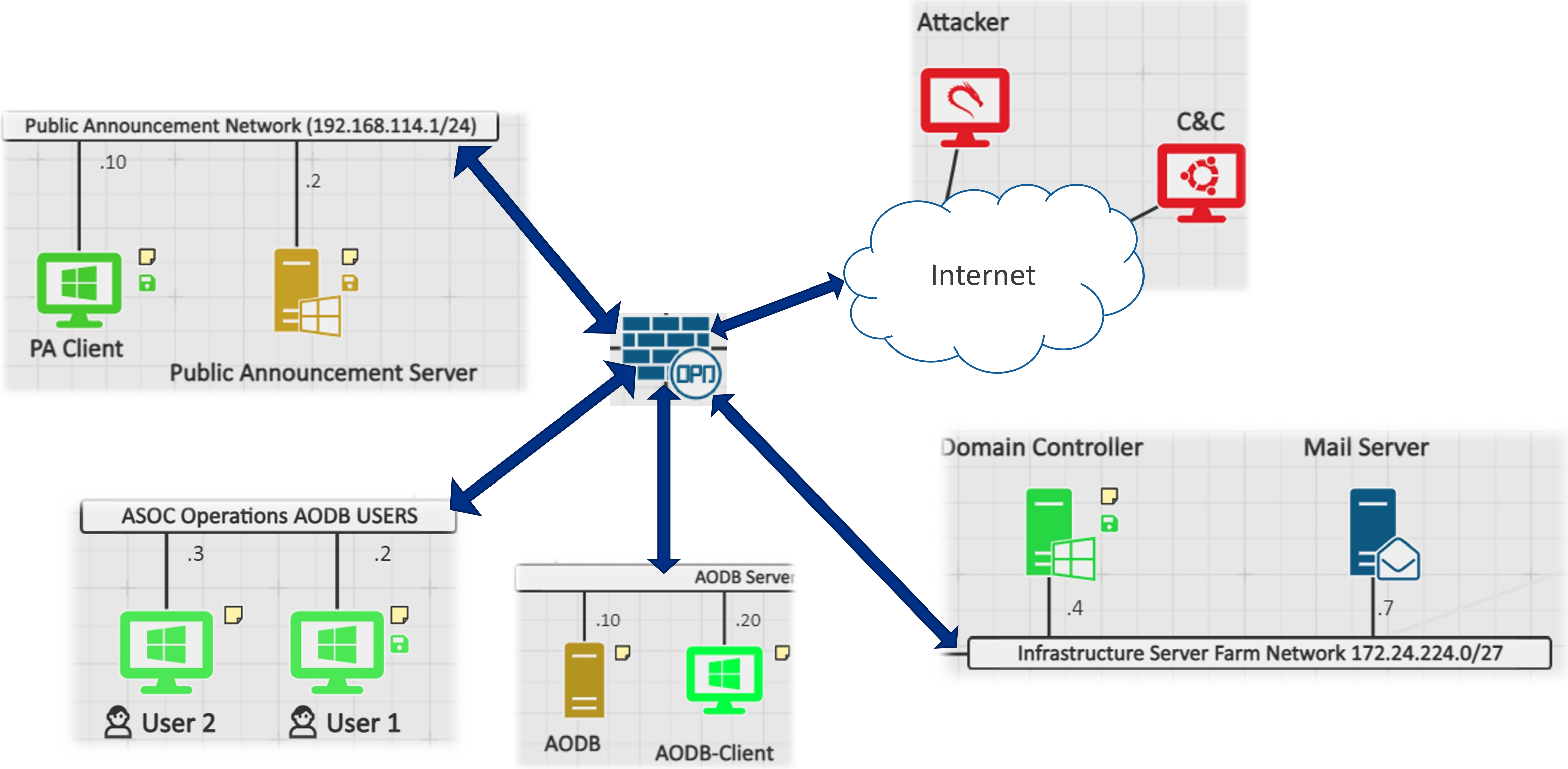
- Cybersecurity Awareness (beginners)
- Intermediate Cybersecurity (intermediate)
- Cybersecurity Professional (advanced)

FORESIGHT Certifications on each domain



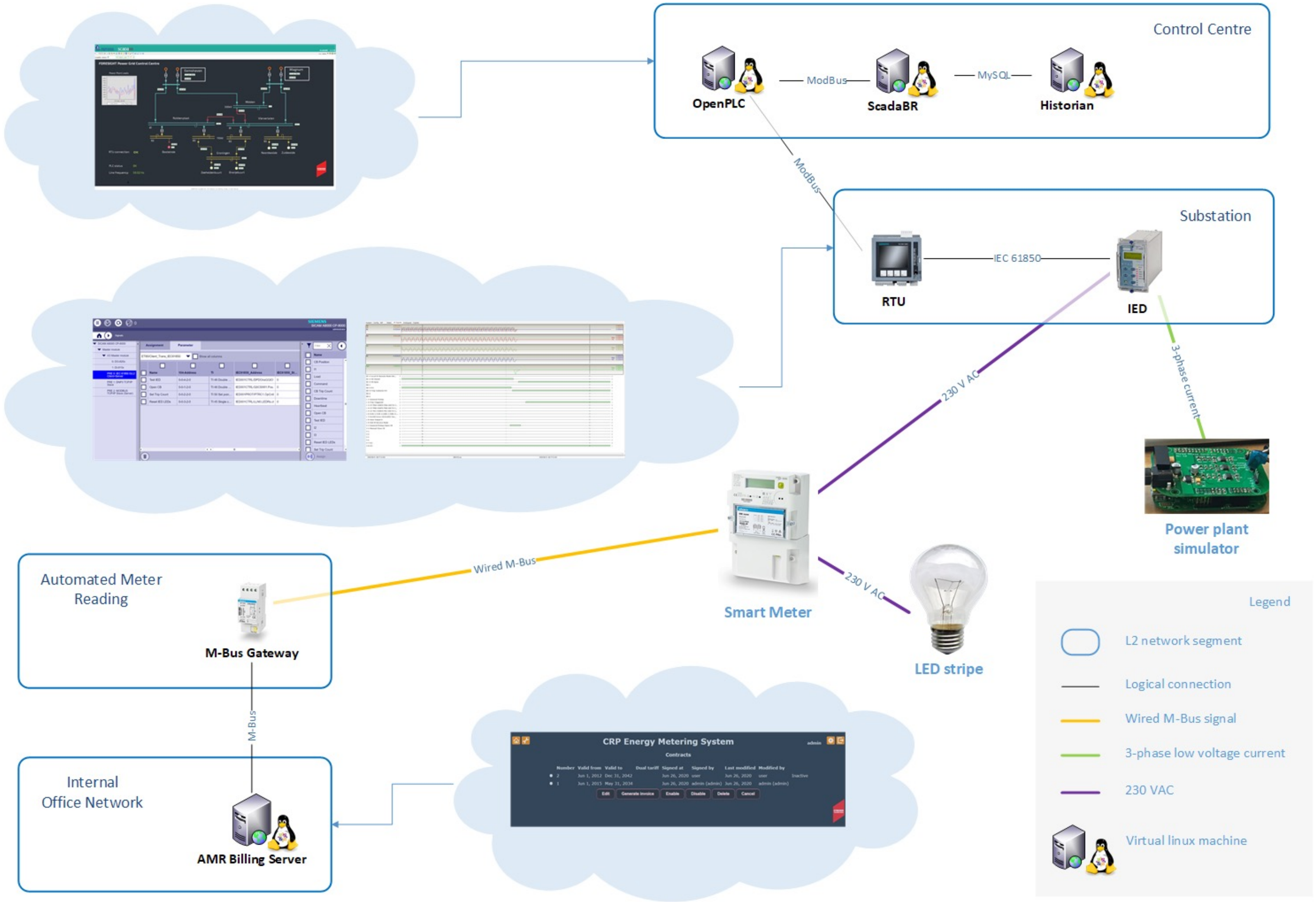
Example Use Case (Aviation)

Advanced Persistent Threats


Attacker
C&C
Internet
Public Announcement Network (192.168.114.1/24)
.10
.2
PA Client
Public Announcement Server
OPN
Domain Controller
Mail Server
.4
.7
Infrastructure Server Farm Network 172.24.224.0/27
ASOC Operations AODB USERS
.3
.2
User 2
User 1
AODB Server
.10
.20
AODB
AODB-Client

Example Use Case (Power Grid)

Replay / data integrity attacks



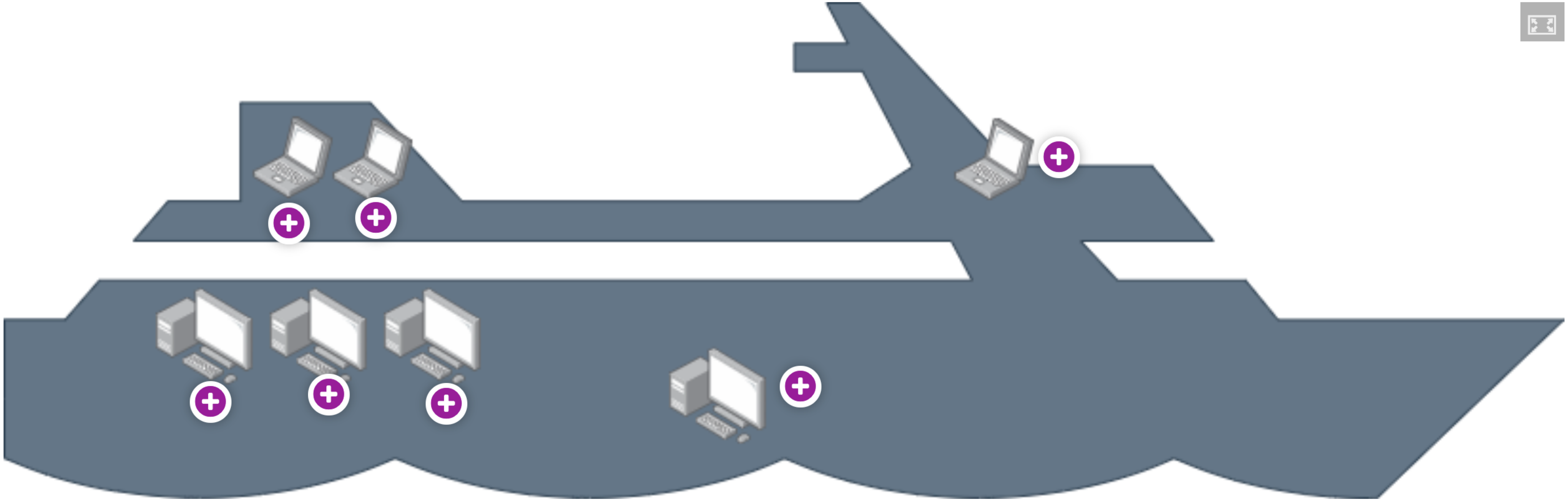
CRP Energy Metering System

Contracts

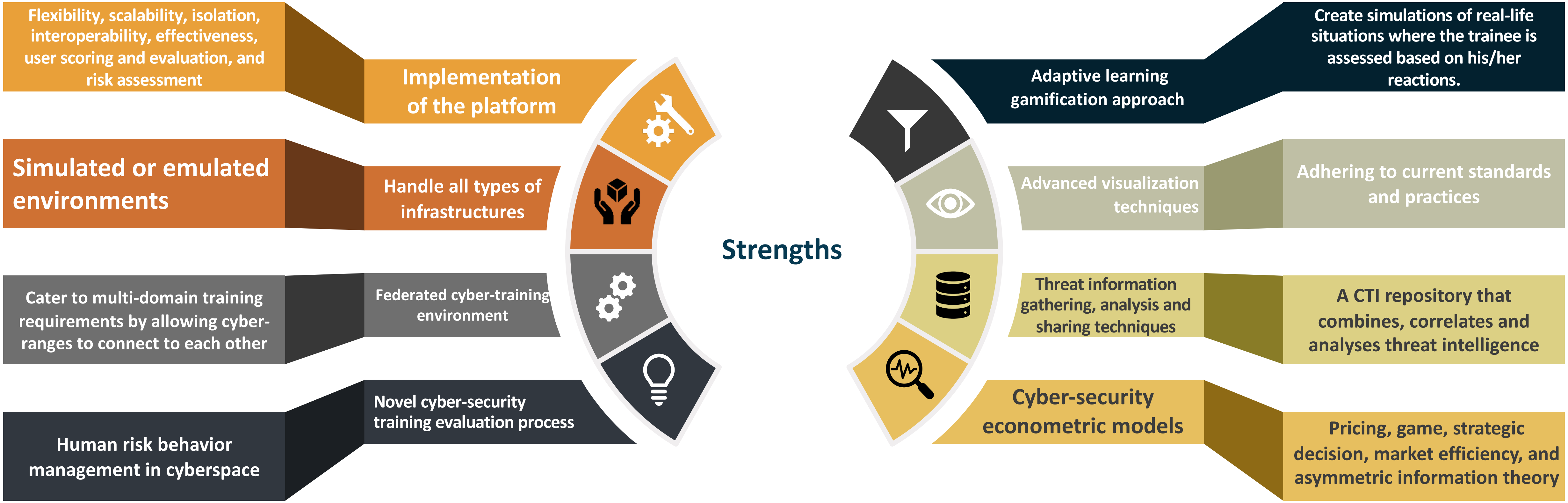
	Number	Valid from	Valid to	Dual tariff	Signed at	Signed by	Last modified	Modified by	
●	2	Jun 1, 2012	Dec 31, 2042		Jun 26, 2020	user	Jun 26, 2020	user	Inactive
●	1	Jun 1, 2015	May 31, 2034		Jun 26, 2020	admin (admin)	Jun 26, 2020	admin (admin)	

Example Use Case (Naval)

Malware Spreading



FORESIGHT Innovation potential



Flexibility, scalability, isolation, interoperability, effectiveness, user scoring and evaluation, and risk assessment

Implementation of the platform

Simulated or emulated environments

Handle all types of infrastructures

Cater to multi-domain training requirements by allowing cyber-ranges to connect to each other

Federated cyber-training environment

Human risk behavior management in cyberspace

Novel cyber-security training evaluation process

Strengths

Create simulations of real-life situations where the trainee is assessed based on his/her reactions.

Adaptive learning gamification approach

Adhering to current standards and practices

Advanced visualization techniques

A CTI repository that combines, correlates and analyses threat intelligence

Threat information gathering, analysis and sharing techniques

Pricing, game, strategic decision, market efficiency, and asymmetric information theory

Cyber-security econometric models

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