FORESIGHT project: Concept, objectives and Results

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

George Kokkinis, *Project Coordinator*

Center For Security Studies (Kentro Meleton Asfaleias – KEMEA)

Cyber-MAR Piraeus Final Pilot Event

16/12/2022

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

Consortium

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

THALES

РАЗПРЕДЕЛЕНИЕ

CERT.BG COMPUTER EMERGENCY RESPONSE TEAM BULGARIA

ieit

ESO

University of Strathclyde Glasgow

UNIVERSITY OF PORTSMOUTH

Project Interactions

2022

Joint Webinar
Cyber-Security challenges and future perspectives

AGENDA

Cyber-Security challenges and future perspectives

Date: Tuesday 18.01.2022

Time: 10.00 – 12.30 CET

Venue: Online Event

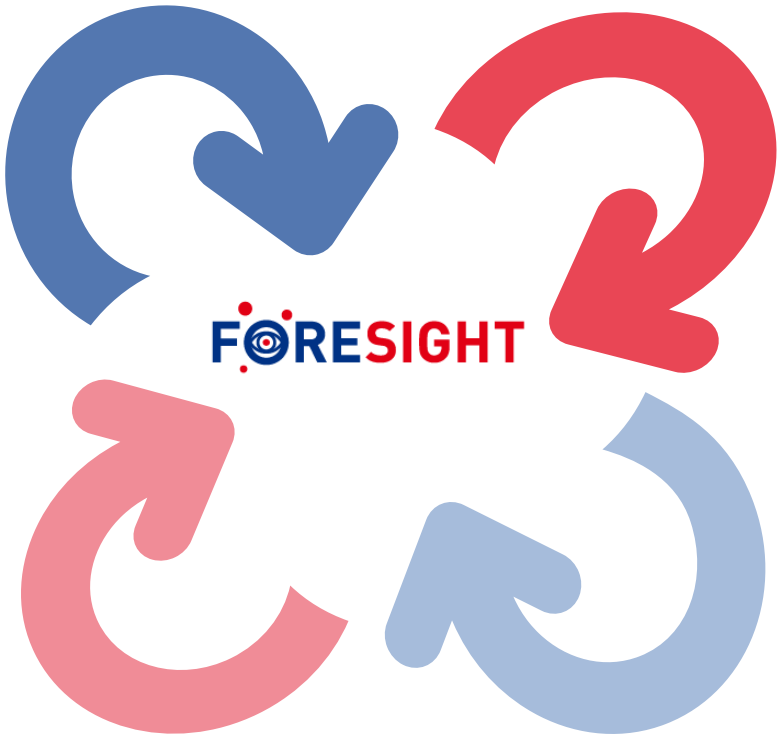
Host: Zoom

Link to the registration form: https://www.eventbrite.com/e/webinar-cyber-security-challenges-and-future-perspectives-tickets-240940017077

Session time slot	Session title	Presenter
10.00 – 10.10	Welcome and Introduction	Moderator **Davide Stasi** Manager Director, International Maritime Safety Security and Environment Academy (IMSSEA) **Aykut I. Ölçer** Director of Research, World Maritime University (WMU) **Vasilis Kassouras** Center for Security Studies (KEMEA) - FORESIGHT Coordinator
10.10 – 10.40	Projects' overview CYBER-MAR project: Concept, objectives and current progress FORESIGHT project: Concept, objectives and current progress	**Eleftherios Ouzounoglou** Institute of Communication & Computer Systems (ICCS) - Cyber-MAR coordinator **Nicholas Kolokotronis** University of the Peloponnese (UOP) – FORESIGHT Technical Manager
10.40 – 11.50	Keynote speeches Practical preparations to counter cyber-attacks at sea Precis IMO documentation and circulars relating to cyber security EU Coastguards Cybersecurity initiatives BREAK (15 min) Aviation Focus Hellenic Electricity Power Grid Focus	**Peter Adams** Special Advisor to the Secretary-General on Maritime Security Maritime Safety Division (IMO) **Bruno Bender** Chairman of the EU Coastguards Functional Forum Cybersecurity working group and National cybersecurity coordinator for the Maritime sector in France **Ricardo De Sousa** ENISA **D. Michalopoulos** Distribution Network Operator S.A
11.50 – 12.30	Conclusions session Round table discussion Q&A Closing remarks	All Moderator **Vasilis Kasouras** Center for Security Studies (KEMEA) - FORESIGHT Coordinator
End of meeting		

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 *additional security measures*
- ✓ Security technology market fragmentation in cyber-defense systems
  - ❖ Security skills' shortage
  - ❖ Lack of security executives' deep awareness of cyber-security risks

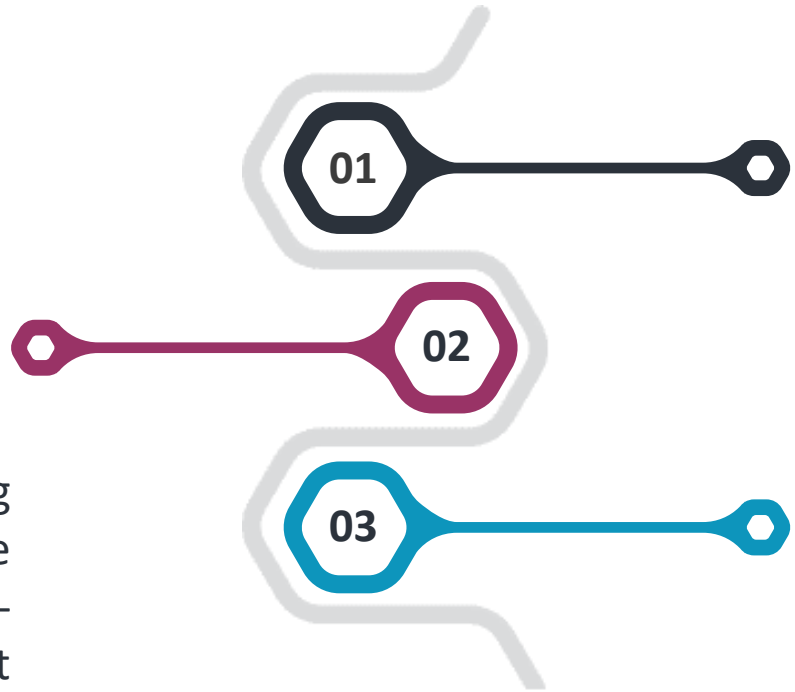


- ✓ Highly skilled cyber-security professionals are needed by the industry
- ✓ Cyber security training should be a continuous learning process
- ✓ Advancements in realistic, diverse, and dynamic simulation environments

FORESIGHT scope

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 cyber-security 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 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.

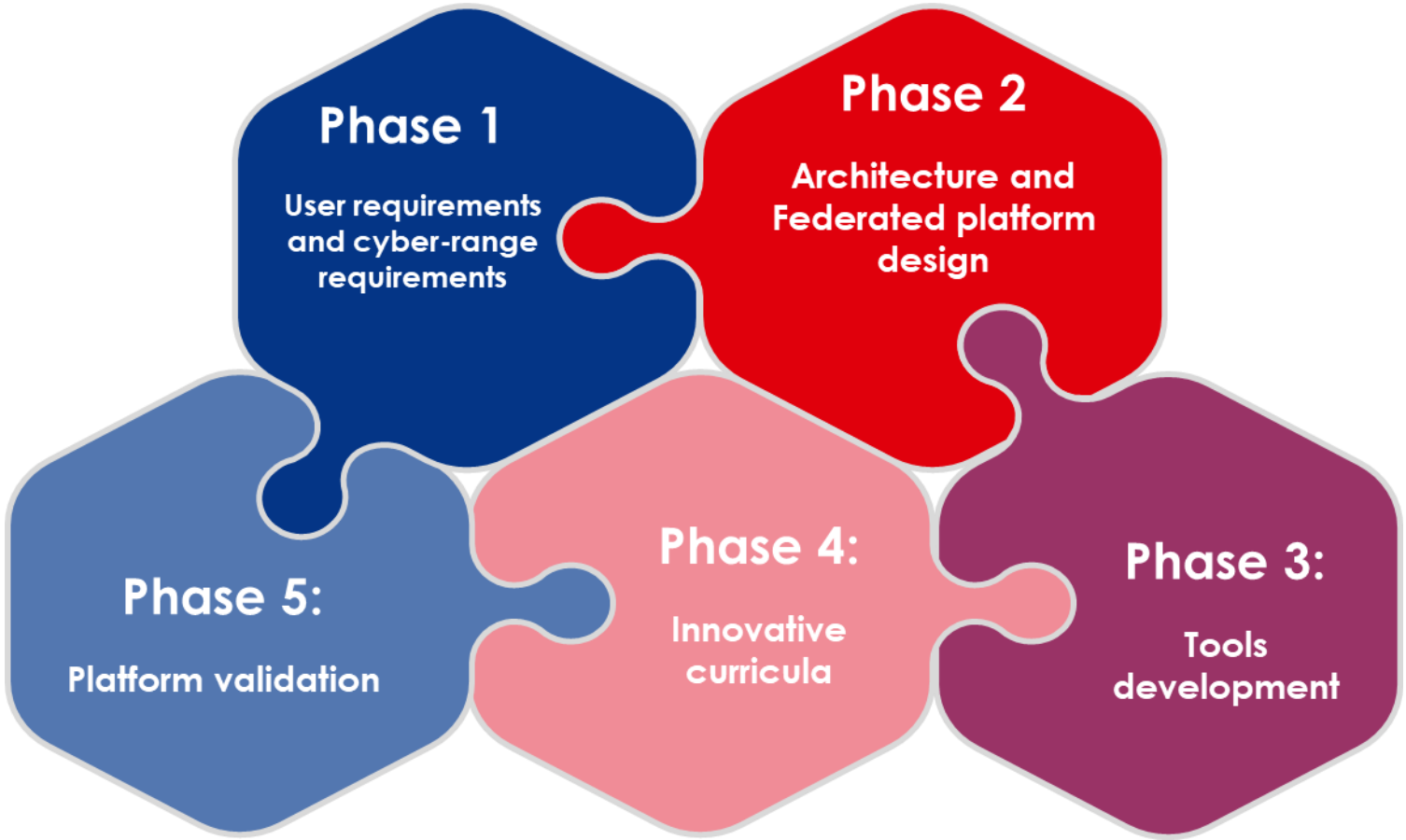
INCREASE the dynamics of training and awareness methods in order to match or even exceed the rate of evolution of cyber-attackers.

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).

FORESIGHT methodology

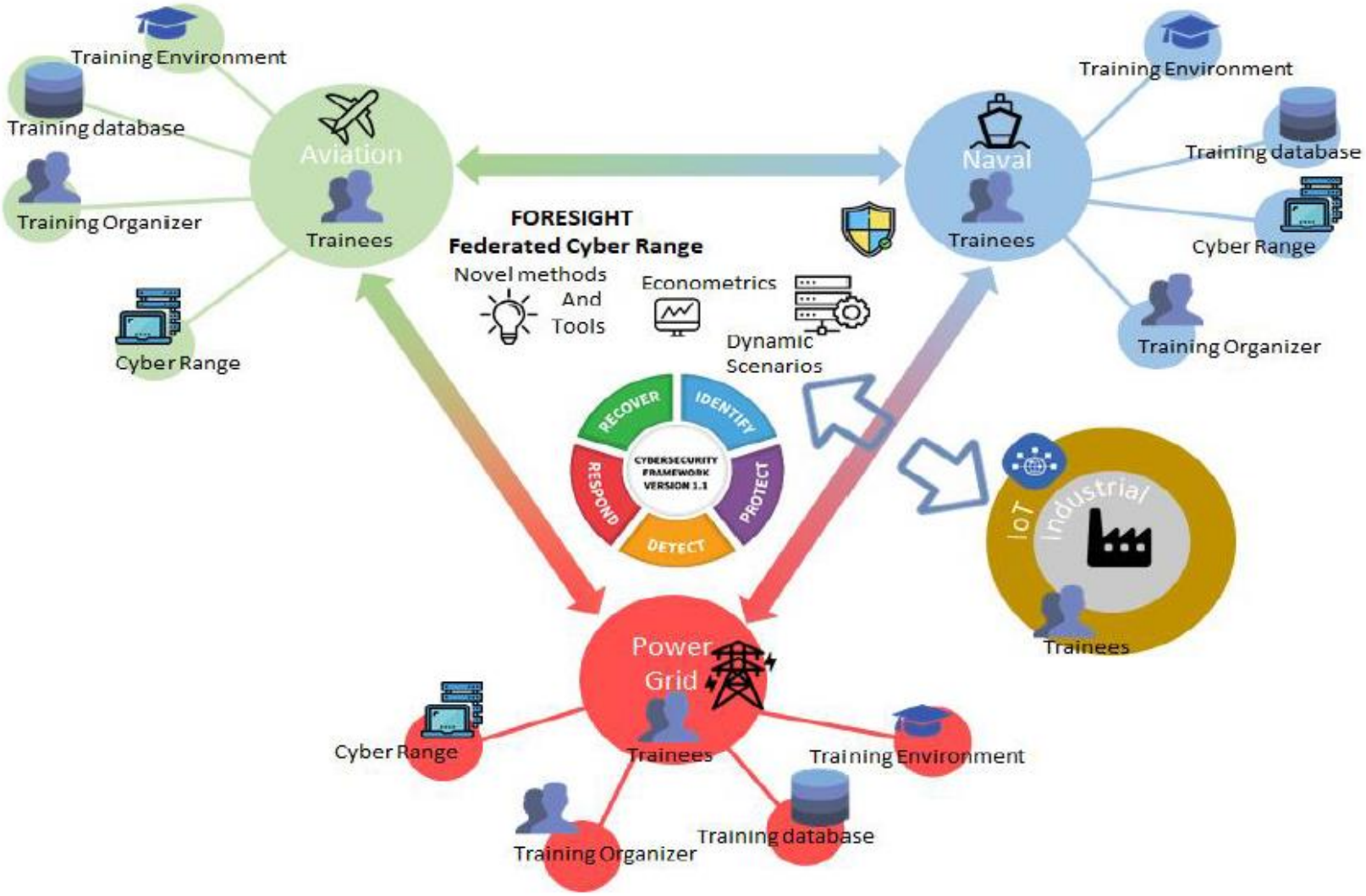
Requirements → Architecture → Development of tools and training material → Validation



FORESIGHT high-level concept

Three vertical Domains formed a hybrid ecosystem

- **Aviation**
- **Power grid**
- **Naval**
- **Hybrid/IoT**



FORESIGHT federation platform for CRs/TEs

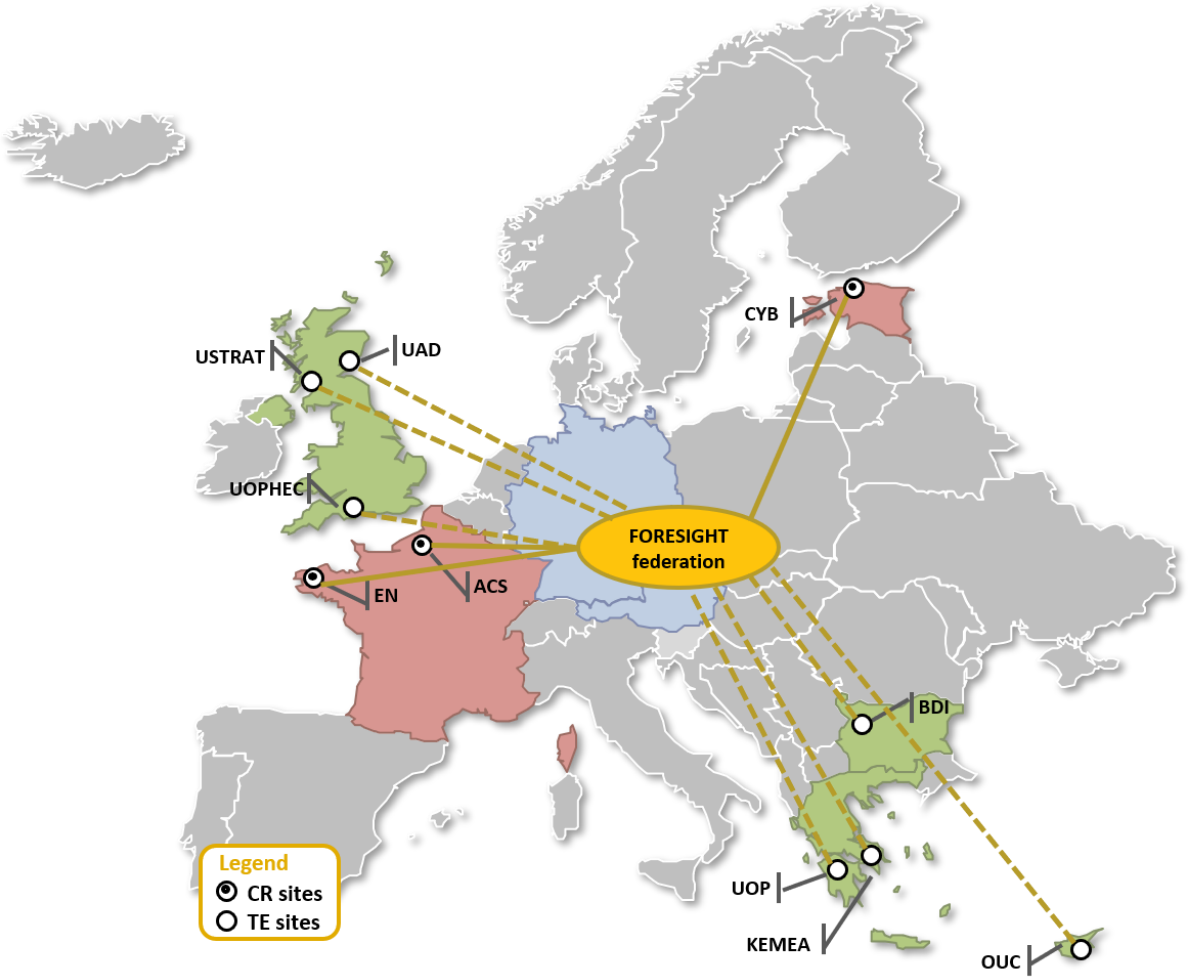
Training Assets for Naval, Aviation and Power Grid

FORESIGHT CRs

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

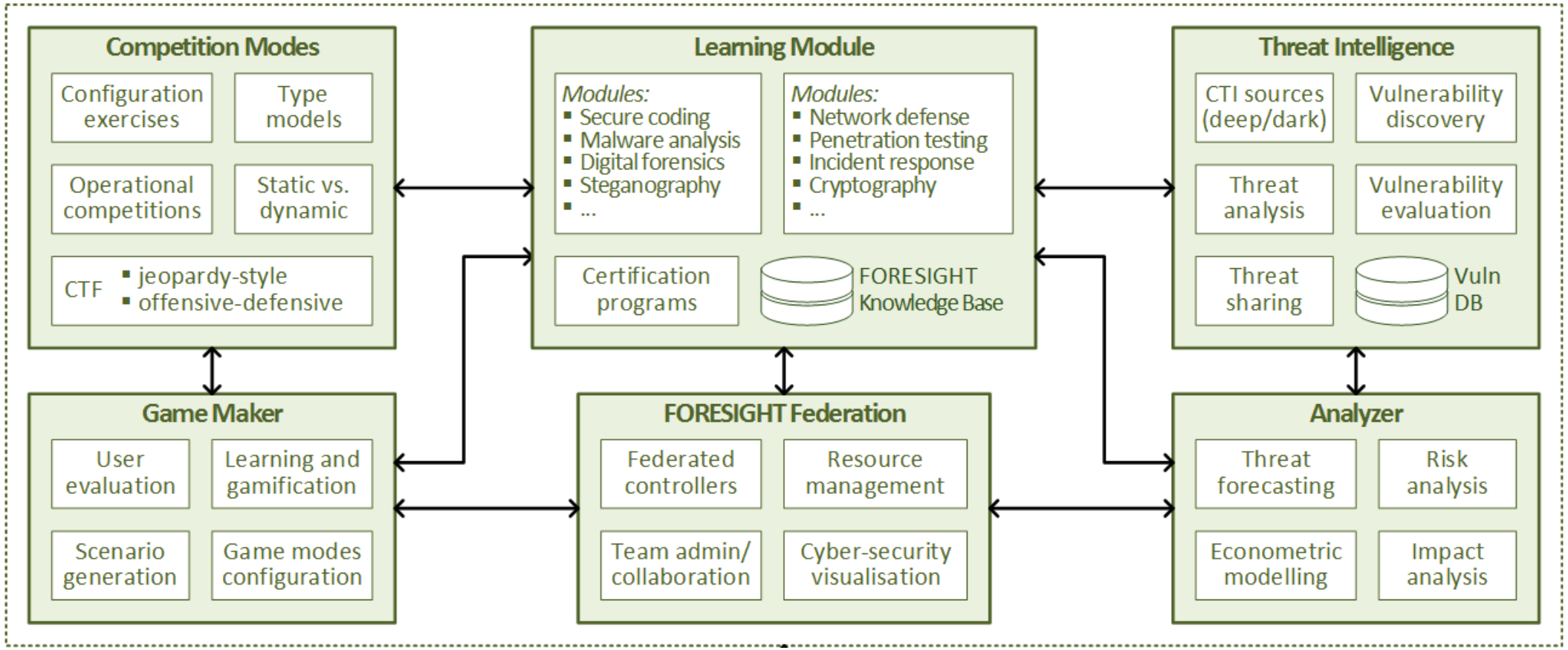
FORESIGHT TEs

- 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

Training is at the center of Foresight



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

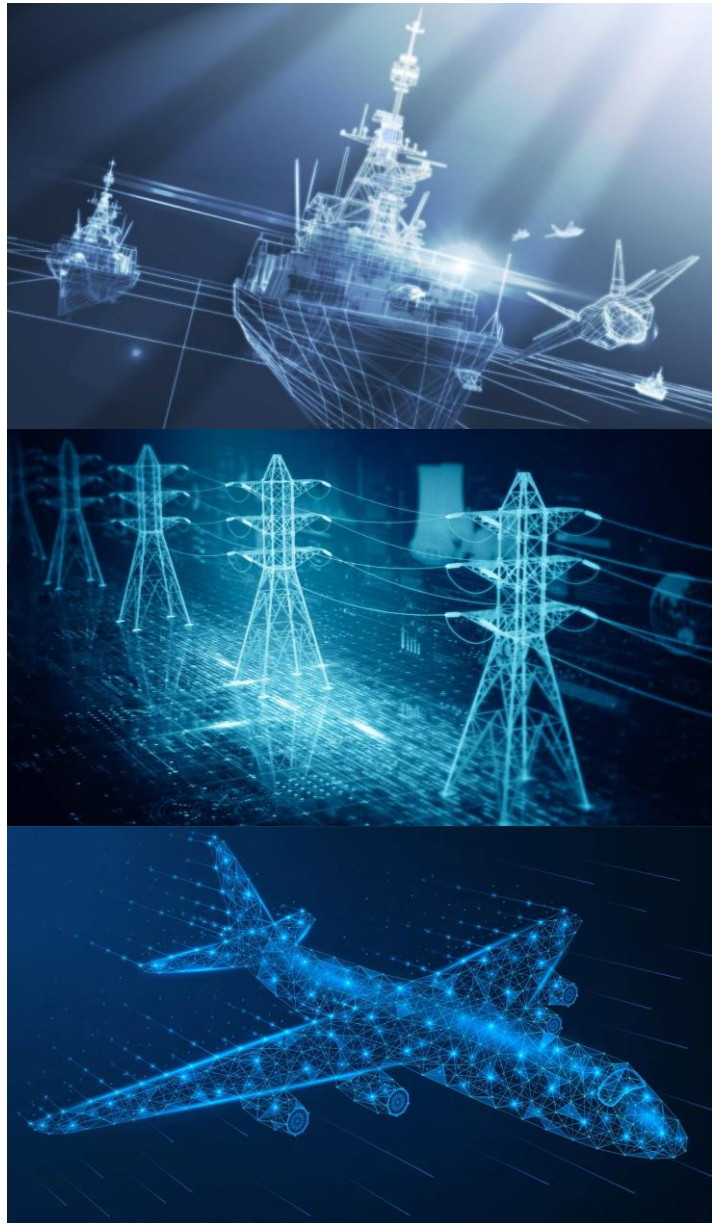
– Different training models	– Multi-faceted approach to cyber-security
– Varying difficulty levels	– Certification based on standards
– Real-world attack scenarios	– Scalable, cost-effective, easy to use programs

FORESIGHT Training and Certification

Learning paths and certifications for the 3domains and a general (focus oriented) learning path

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

- Learning Path 1 **Naval**
  (2 levels, 7 modules)
  - CAN – Cybersecurity Awareness Naval, (Beginner Level)
  - ICN – Intermediate Cybersecurity Naval (Intermediate Level)
- Learning Path 2 **Power Grid**
  (3 levels, 12 modules)
  - CAP – Cybersecurity Awareness Power Grid (Beginner Level)
  - ICP – Intermediate Cybersecurity Power Grid (Intermediate Level)
  - CPP – Cybersecurity Professional Power Grid (Advanced Level)
- Learning Path 3 **Aviation**
  (3 levels, 7 modules)
  - CCA – Cybersecurity Common Aviation (Beginner Level)
  - COA – Cybersecurity Operator Aviation (Intermediate Level)
  - CAA – Cybersecurity Analyst Aviation (Advanced Level)
- Learning Path 4 **General**
  (7 courses, 34 modules)



FORESIGHT Certification Programme

FORESIGHT Credits Policy

ECTS: European Credit Transfer and Accumulation System

“express the volume of learning based on the defined learning outcomes and their associated workload (the time the trainees typically needs to complete all learning activities such as classes, projects, practical labs, training exercises)”

ECVET: European Credit System for Vocational Education and Training

“allows learners to accumulate, transfer and use their learning in units as these units are achieved”

Building qualifications at learners’ own pace from learning outcomes

The system is based on units of learning outcomes as part of qualifications that can be assessed and validated.

It applies to VET (Vocational Education and Training) qualifications at all levels of the European Qualifications Framework (EQF)

CAN - Cybersecurity Awareness Naval Credits: 0.48 ECTS / 0.72 ECVET

ICN – Intermediate Cybersecurity Naval Credits: 0.80 ECTS / 1.20 ECVET

- Valid for three years
- **Renewal policy**: After expiration, renewal can be done either by passing the current version of the exam or by submitting 0.40 ECTS number of credits within a year.

Cost: Cost: 875€ + 1625€

FORESIGHT Naval Training

Overview

Naval Training

Learning Path

Technical competencies

1. Web security
2. Network security
3. Software security
4. Malware analysis
5. Internet of Things
6. Reverse Engineering
7. Digital Forensics
8. Cryptography

Critical Thinking

How SOPs can be applied to specific trainees' job.
How to instantiate and deploy the method on a maritime bid or project, covering:

a. preparation activities, including system architecture documentation gathering;
b. planning and organization of sessions;
c. tooling aspects;
d. Cyber Maritime internal community resources.

What are the limits of risk analysis and its application to the maritime domain?
How these cyberattacks and the monitoring could influence the trainees' day-to-day work.

List of courses and module

N1 – Basic Concepts of Cybersecurity
N2 – Cybersecurity in Naval Domain
N3 – Ship and Crew Cybersecurity
N4 – Maritime Cybersecurity SOPs Best Practices
N5 – Cybersecurity Risk Assessment (optional)
N6 – Basic Concepts of Cryptography, Digital Forensics and Network Security (optional)
N7 – Maritime Cybersecurity Applications

Analytical skills

- Identifying basic cases of cyber-attacks
- Identifying normal vs. abnormal situations on-board
- Running a risk assessment and risk treatment on a maritime example
- Monitoring the behaviour of the operational system
- Investigating basic (known) attacks
- Applying some cybersecurity operational procedures and toolset in practical cases of cyber-attacks

FORESIGHT Naval Training

Beginner and Intermediate level

Cybersecurity Awareness for Naval (CAN) Courses

Module	Level	Prerequisites	Hrs	Evaluation
N1. Basic concepts of cybersecurity	Beg		2.5	Questionnaire
N2. Cybersecurity in naval domain	Beg	N1	2.5	Questionnaire
N3. Ship and crew cybersecurity	Beg	N2	3	Hands-on: cyber-range
N4. Maritime cybersecurity SOP best practices	Beg	N3	4	Hands-on: cyber-range

Intermediate Cybersecurity for Naval (ICN) Courses

Module	Level	Prerequisites	Hrs	Evaluation
N5. Cybersecurity risk assessment[optional]	Int	N4	8	Questionnaire
N6. Basic concepts of cryptography, digital forensics and network security[optional]	Int	N4	8.5	Questionnaire
N7. Maritime cybersecurity applications	Int	N4–6	4	Hands-on: cyber-range

Basic Concepts of Cybersecurity

Module N1

Learning outcomes

At the end of this module, the trainees will be able to define the main terms used in cybersecurity.

Knowledge

- The CIA triad (Confidentiality / Privacy, Integrity, Availability)
- IAAA (Identification, Authentication, Authorisation, Accountability).
- Security versus safety (a clarification).

Analytical skills

N/A

Critical thinking

N/A

Detailed syllabus

A lecture will provide definitions of basic security concepts:The CIA triad and IAAA

Assessment

The assessment consists of simple quizzes. A questionnaire will be provided prior to the training, to assess prior knowledge, but also to push the trainees to reflect about the key cybersecurity concepts.

Cybersecurity in Naval Domain

Module N2 [Prerequisite N1]

Learning outcomes

Citing the maritime-relevant threats, actors, and their motives, together with examples of cyber-attacks on OT/IT systems

Knowledge

- Taxonomies of threats
- Maritime-relevant threats, actors, and their motives
- Examples of cyber-attacks on naval-relevant OT/IT systems

Analytical skills

Basics for being able to execute a risk assessment

Critical thinking

N/A

Detailed syllabus

Cybersecurity domain introduction; Cyber elements in maritime domain; Inter domain, Multi domain and Transversal domain cybersecurity aspects

Assessment

The assessment consists of questionnaires and the opportunity given to the trainees to make presentations of their lessons learnt, based on field experience.

Ship and Crew Cybersecurity

Module N3 [Prerequisite N2]

Learning outcomes

Identify cyber-attacks occurring and measure the consequences of the attacks on different subsystems of a ship

Knowledge

- Trainees will observe typical examples of impacts of a cyber-attacks during their normal day-to-day activity, in order to understand the importance and need for cybersecurity.
- The close-to-reality situations run on the naval cyber-range will include: - *ship in maintenance, with technical staff* and *ship in port or at sea, with captain and crew*

Analytical skills

Identify normal/abnormal situations on-board

Critical thinking

Analyse how these attacks could influence the trainees' day-to-day work.

Detailed syllabus

Cognitive and technical aspects of cybersecurity, Cyberattack taxonomy, Best practices of cyber hygiene.

Assessment

The assessment consists of quizzes, questionnaires and the opportunity given to the trainees to provide feedback on what they have just seen in relation with their experience in the field.

Maritime Cybersecurity SOPs Best Practices

Module N4 [Prerequisite N3]

Learning outcomes

Apply best cyber security practices on-board

Knowledge

Maritime-relevant regulatory frameworks, SOPs, best practices and basic cyber-hygiene which can be used to prevent and mitigate the attacks seen in N2 and N3.

Analytical skills

N/A

Critical thinking

Understand how SOPs can be applied to specific trainees' job

Detailed syllabus

Cybersecurity regulatory framework, SOP main concept, Study SOP examples, Developing sample SOPs

Assessment

The assessment consists of debriefing sessions of the project assignments, with possibly some additional questionnaires.

Maritime Cybersecurity SOPs Best Practices

Module N5 [Prerequisite N4] [OPTIONAL]

Learning outcomes

- Know core tenets of the risk management method:
- study and define a security base (Minimal Set of Security Controls)
- identify and sort the relevant risk sources define strategic scenarios
- describe how an attacker may affect the system under study
- define operational scenarios describing in detail how an attacker may affect the system under study, and how likely this attack may be
- ISO 27005 options to treat cybersecurity risks, and how to assess the residual risks

Knowledge

EBIOS – Risk Manager method

Analytical skills

Running a risk assessment and risk treatment on a maritime environment

Critical thinking

Preparation activities, including system architecture documentation gathering, Planning and organisation of sessions, Tooling aspects, Cyber Maritime internal community resources

Knowing the limits of risk analysis and its application to the maritime domain.

Detailed syllabus

Cybersecurity risk assessment introduction, Cybersecurity on board ships guide, Risk assessment exercises

Assessment

The assessment consists of questionnaires and the opportunity given to the trainees to make presentations of their lessons learnt, based on field experience.

Basic Concepts of Cryptography, Digital Forensics and Network Security

Module N6 [Prerequisite N4] [Optional]

Learning outcomes

Perform basic digital forensic investigation.

Knowledge

G5 – Cryptography Fundamentals, G2 – Network Security Fundamentals, G7 – Introduction to Network Forensics and Investigating Logs, G13 – Web Attack Investigations

Analytical skills

Monitoring the behaviour of a system, Investigation of basic (known) attacks

Critical thinking

N/A

Detailed syllabus

Cybersecurity Scenario development, Cybersecurity use cases definitions, Operational procedure assessment with respect to cybersecurity, Identifying and applying cybersecurity tools from existing set of tool

Assessment

The assessment consists of questionnaires and written tests.

Maritime Cybersecurity Applications

Module N7 [Prerequisites N4 and N6]

Learning outcomes

Apply cybersecurity SOPs and use toolset in practical situations of cyber-attacks (a) ship in maintenance, with technical staff; (b) ship in port or at sea, with captain and crew.

Knowledge

N/A

Analytical skills

Monitor the operational system, Identify basic cases of cyber-attacks, Apply cybersecurity SOPs and use tools in practical cases of cyber-attacks.

Critical thinking

Analyse how these attacks and this monitoring could influence the trainees' day-to-day work.

Detailed syllabus

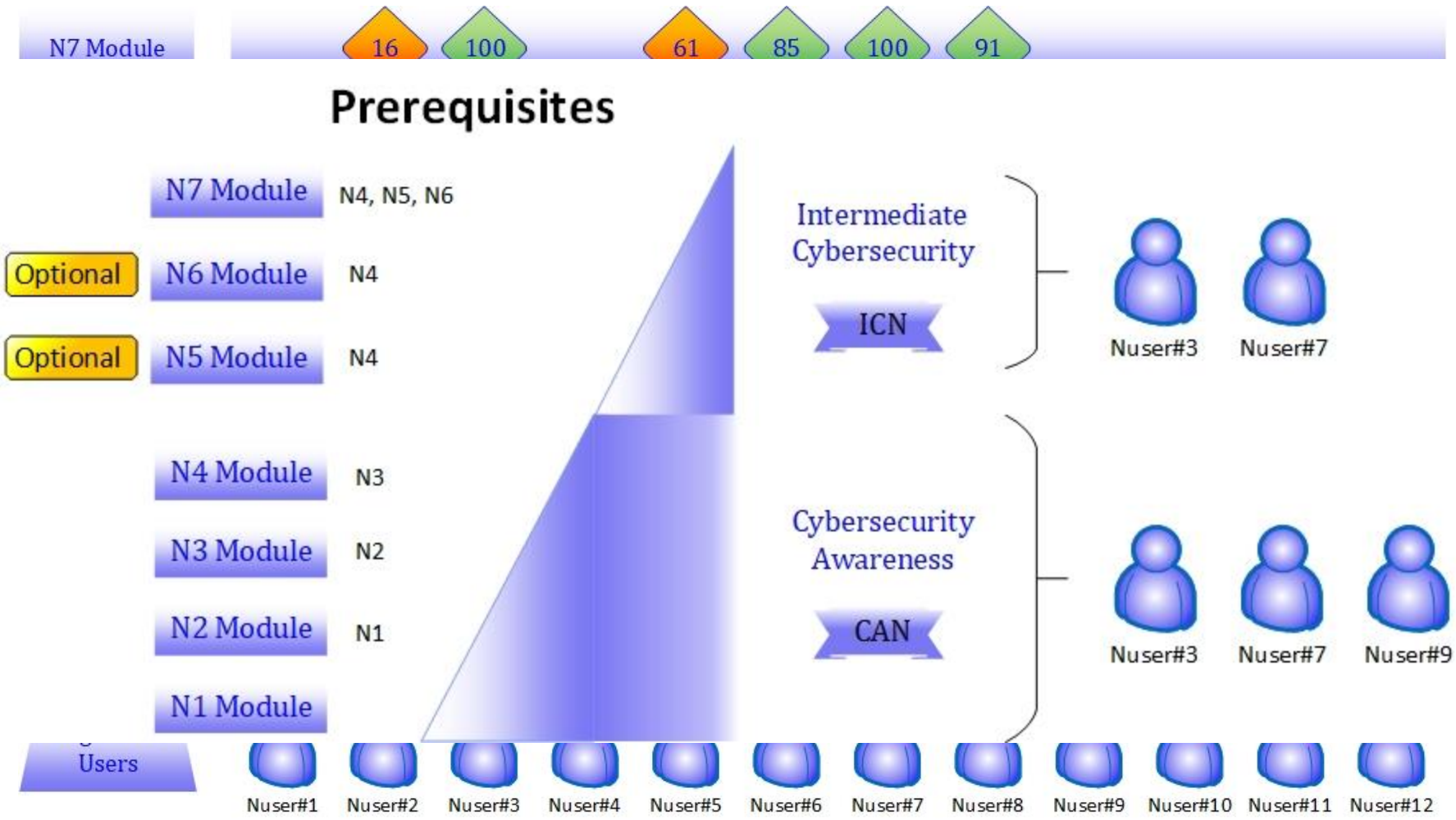
Cyber Security scenario development, Cybersecurity use cases definitions Operational procedure assessment with respect to cybersecurity, Identifying and applying cybersecurity tools from existing set of tools

Assessment

The assessment consists of debriefing sessions about the project assignments, possibly with additional questionnaires.

Foresight Pilots (Naval Specific)

Results



FORESIGHT General Training

Overview

FORESIGHT General Training

Secure Computer User (SCU) Courses

Module	Lvl	Req	Hrs	Evaluation
G1. Web security fundamentals	Beg		4	Questionnaire
G2. Network security fundamentals	Beg		3.5	Questionnaire
G3. Network topology aspects	Beg		3	Questionnaire
G4. Operating systems security fundamentals	Beg		3.5	Questionnaire
G5. Cryptography fundamentals	Beg		4	Questionnaire
G6. Malware fundamentals	Beg		6	Questionnaire
G18. Cryptographic applications	Int	G5	8	Mixed: Hands-on / Quiz

FORESIGHT General Training

Web Security Developer (WSD) Courses

Module	Lvl	Req	Hrs	Evaluation
G1. Web security fundamentals	Beg		4	Questionnaire
G12. Reverse engineering fundamentals	Int		5	Mixed: Hands-on / Quiz
G16. Code review	Int	G14	5	Mixed: Hands-on / Quiz
G18. Cryptographic applications	Int	G5	8	Mixed: Hands-on / Quiz
G20. Cross-site scripting vulnerabilities	Int		3	Mixed: Hands-on / Quiz
G21. Cross-site request forgery vulnerabilities	Int		3	Mixed: Hands-on / Quiz
G27. Preventing SQL injections	Int		4	Mixed: Hands-on / Quiz
G28. Cookies manipulation	Int		3	Mixed: Hands-on / Quiz

FORESIGHT General Training

Penetration Tester (PEN) Courses

Module	Lvl	Req	Hrs	Evaluation
G19. SQL injection attacks	Int		6	Mixed: Hands-on / Quiz
G20. Cross-site scripting vulnerabilities	Int		3	Mixed: Hands-on / Quiz
G21. Cross-site request forgery vulnerabilities	Int		3	Mixed: Hands-on / Quiz
G22. Network penetration testing	Int	G7	7	Mixed: Hands-on / Quiz
G28. Cookies manipulation	Int		3	Mixed: Hands-on / Quiz
G30. Password attacks	Int	G4	4	Mixed: Hands-on / Quiz
G33. Social engineering	Adv	G8	5	Mixed: Hands-on / Quiz

FORESIGHT General Training

Digital Forensics Investigator (DFI) Courses

Module	Lvl	Req	Hrs	Evaluation
G7. Introduction to network forensics and log investigation	Beg		4	Mixed: Hands-on / Quiz
G11. Static analysis tools & methodologies	Beg		10	Mixed: Hands-on / Quiz
G13. Web attack investigations	Int	G1	5	Mixed: Hands-on / Quiz
G23. Dynamic analysis tools & methodologies	Int	G11	5	Mixed: Hands-on / Quiz
G31. Incident response	Adv		1	Questionnaire
G32. Investigating networks and devices	Adv	G1, 2	6	Mixed: Hands-on / Project

FORESIGHT General Training

Cyber Security Engineer (CSE) Courses

Module	Lvl	Req	Hrs	Evaluation
G1. Web security fundamentals	Beg		4	Questionnaire
G3. Network topology aspects	Beg		3	Questionnaire
G8. Offensive and defensive mechanisms	Beg	G14	6	Questionnaire
G10. Radio communication protocols security	Beg		3	Questionnaire
G14. Vulnerabilities and security tools	Int	G22	4.5	Mixed: Hands-on / Quiz
G15. Operating system hardening	Int		10	Mixed: Hands-on / Quiz
G17. App hardening and malware detection	Int	G15	6	Questionnaire
G26. Preparedness for network attacks	Int	G22	6	Questionnaire
G29. Network defence and attack assessments	Int	G9	4	Mixed: Hands-on / Quiz
G30. Password attacks	Int	G4	4	Mixed: Hands-on / Quiz
G33. Social engineering	Adv	G8	5	Mixed: Hands-on / Quiz

FORESIGHT General Training

Information Security Administrator (ISA) Courses

Module	Lvl	Req	Hrs	Evaluation
G1. Web security fundamentals	Beg		4	Questionnaire
G3. Network topology aspects	Beg		3	Questionnaire
G9. Threats, endpoints and monitoring	Beg		3	Questionnaire
G17. App hardening and malware detection	Int	G15	6	Mixed: Hands-on / Quiz
G18. Cryptographic applications	Int	G5	8	Mixed: Hands-on / Quiz
G24. Web applications and security controls	Int	G1	4	Mixed: Hands-on / Quiz
G26. Preparedness for network attacks	Int	G22	6	Questionnaire
G27. Preventing SQL injections	Int		4	Mixed: Hands-on / Quiz

FORESIGHT General Training

Information Security Administrator (ISA) Courses

Module	Lvl	Req	Hrs	Evaluation
G1. Web security fundamentals	Beg		4	Questionnaire
G3. Network topology aspects	Beg		3	Questionnaire
G9. Threats, endpoints and monitoring	Beg		3	Questionnaire
G17. App hardening and malware detection	Int	G15	6	Mixed: Hands-on / Quiz
G18. Cryptographic applications	Int	G5	8	Mixed: Hands-on / Quiz
G24. Web applications and security controls	Int	G1	4	Mixed: Hands-on / Quiz
G26. Preparedness for network attacks	Int	G22	6	Questionnaire
G27. Preventing SQL injections	Int		4	Mixed: Hands-on / Quiz

FORESIGHT General Training

Cyber Security Analyst (CSA) Courses

Module	Lvl	Req	Hrs	Evaluation
G7. Introduction to network forensics and log investigation	Beg		4	Mixed: Hands-on / Quiz
G8. Offensive and defensive mechanisms	Beg	G14	6	Questionnaire
G11. Static analysis tools and methodologies	Beg		10	Mixed: Hands-on / Quiz
G12. Reverse engineering fundamentals	Int		5	Mixed: Hands-on / Quiz
G13. Web attack investigations	Int	G1	5	Mixed: Hands-on / Quiz
G14. Vulnerabilities and security tools	Int	G22	4.5	Mixed: Hands-on / Quiz
G23. Dynamic analysis tools & methodologies	Int	G11	5	Mixed: Hands-on / Quiz
G25. Threat analysis and modelling	Int	G9	6	Project
G29. Network defence and attack assessments	Int	G9	4	Mixed: Hands-on / Quiz
G31. Incident response	Adv		1	Questionnaire
G32. Investigating networks and devices	Adv	G1, 2	6	Mixed: Hands-on / Project
G34. Threat evaluation	Adv	G9, G14	4	Questionnaire

George Kokkinis - KEMEA

g.kokkinis@kemea-research.gr