ESA SECURITY

SECURITY CYBER CENTRE of EXCELLENCE (SCCoE)

John Irving

Jean Luc Trullemans

Gioacchino Buscemi

14/05/2021

V1.11

AGENDA

1. ESA in Security Context
2. What is a CoE ?
3. What is the ESA SCCoE ?
4. ESA Roadmap for the ESA SCCoE?
5. Getting onboard

AGENDA

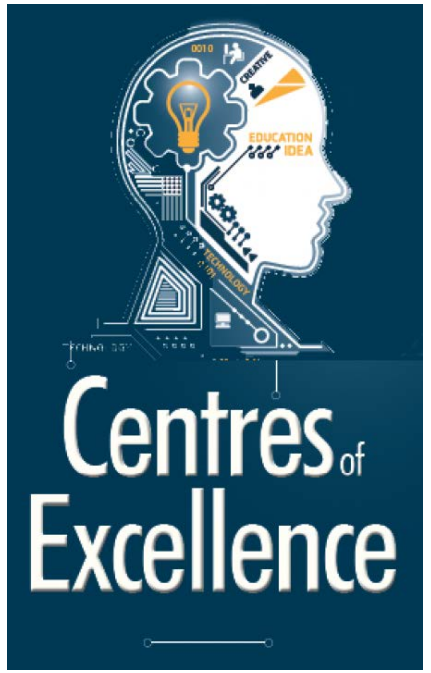
1. ESA in Security Context
2. What is a CoE ?
3. What is the ESA SCCoE ?
4. ESA Roadmap for the ESA SCCoE?
5. Getting onboard

WHAT IS A CENTRE of EXCELLENCE ?

CENTRE of EXCELLENCE ?

Brings together different disciplines for share facilities/resources

- *“A team, shared facility or entity that provides leadership, best practices, research, support and/or training for a focus area” [wikipedia]*
- *“Concentrating existing expertise & resources in a discipline or capability to attain & sustain world-class performance & value” [Gartner]*

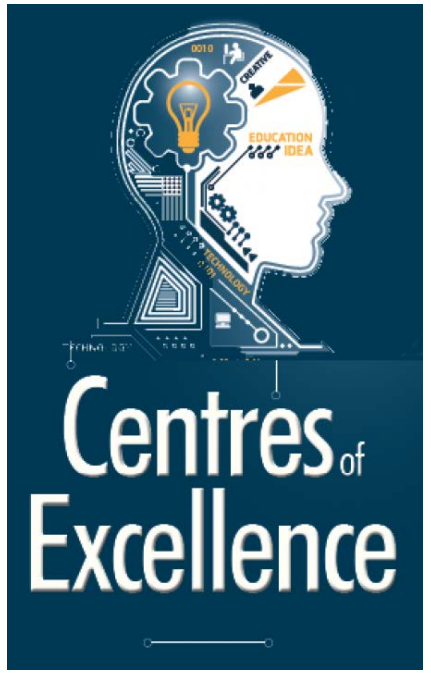


Source : Image ITU

CENTRE of EXCELLENCE ?

Focus on

- Providing *thought* leadership and direction
- Establishing and promoting best practices
- Research and development
  - Provide appropriate recommendations
- Support and education
- Optimizing organization or practices
- Identifying and reducing duplication of effort
  [perficient]



Source : Image ITU

WHAT IS A CYBER RANGE?

ENVIRONMENT WITH GROUND AND SPACE SYSTEM EMULATION

COMMON CYBER RANGE DEFINITION

Multipurpose virtual environment in which organisations can test critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their strategic information, services, and assets

ESA SCCoE REFINEMENT

Common definition and information technology (IT) operational technology (OT) **Space**.

Training, testing, research

Threat detection, intelligence, collaboration and automation

ENVIRONMENT WITH GROUND AND SPACE SYSTEM EMULATION

Platform for development, delivery and use of interactive simulation, emulation environments.

Emulation (or simulation) environment is a representation of the organisation's (**ESA/Space**) ICT, OT, mobile and physical systems, applications and infrastructures.

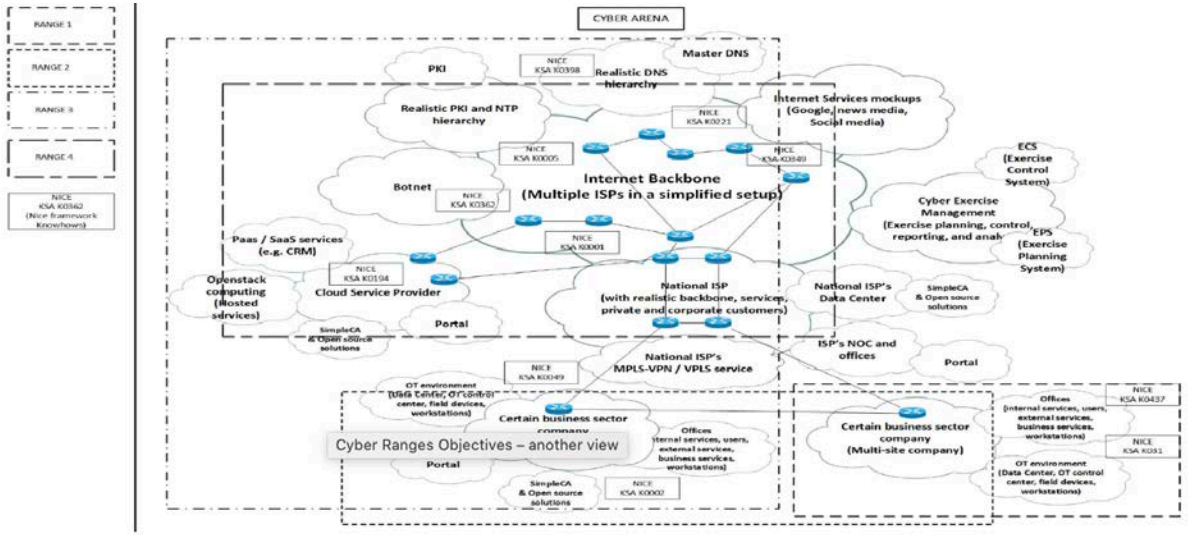
Includes the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the environment may depend upon.

A cyber range includes a combination of core technologies for the realisation and use of the environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases.

CYBER RANGE OBJECTIVES

COMMON OBJECTIVES

- Development of Cyber Resilience & Capabilities
- Research
- Competence Building
- Collaboration between partners



CYBER RANGE OBJECTIVES – ANOTHER VIEW (I)

PROJECT SUPPORT

OPERATIONAL SUPPORT

Evaluate

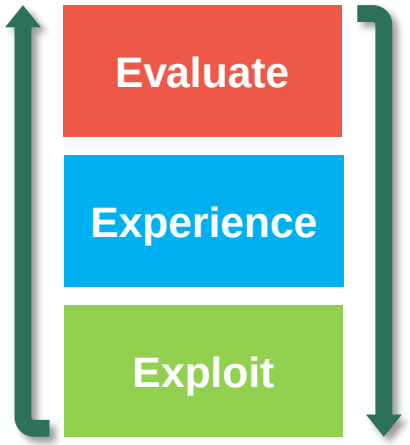
Experience

Exploit

CYBER RANGE OBJECTIVES – ANOTHER VIEW (II)

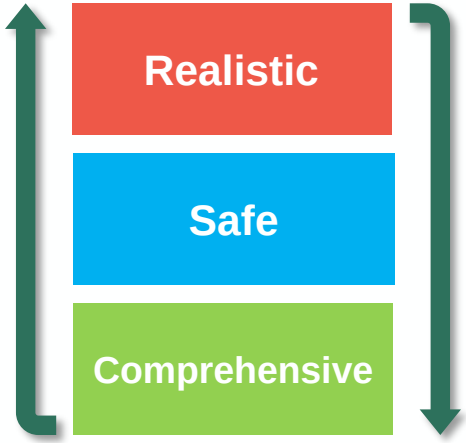
COLLABORATION & PARTNERSHIP

RESEARCH & DEVELOPMENT



CYBER RANGE – WHAT TO LOOK FOR (I)

- Realistic
- Controlled
- Infrastructure model
- Network Simulation/Emulation



CYBER RANGE – WHAT TO LOOK FOR (II)

- System
- traffic generation
- Attack execution

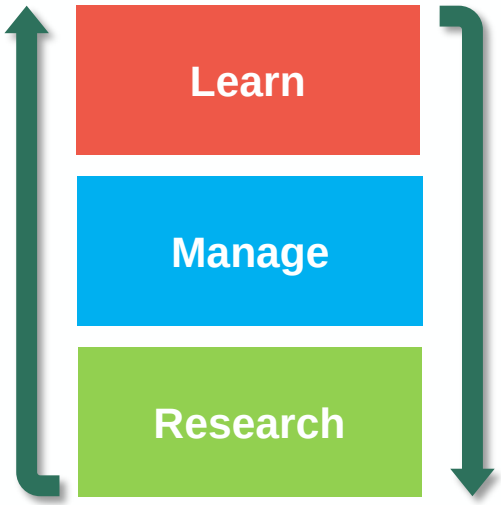
- Collaboration
- Planning, executing, monitoring & analysis
- Accessible & Flexible
- Stable,
- Repeatable,
- Flexible

CYBER RANGE – WHAT TO LOOK FOR (III)

RANGE LEARNING MANAGEMENT SYSTEM

Main Differentiator between a professional cyber range & cyber lab.

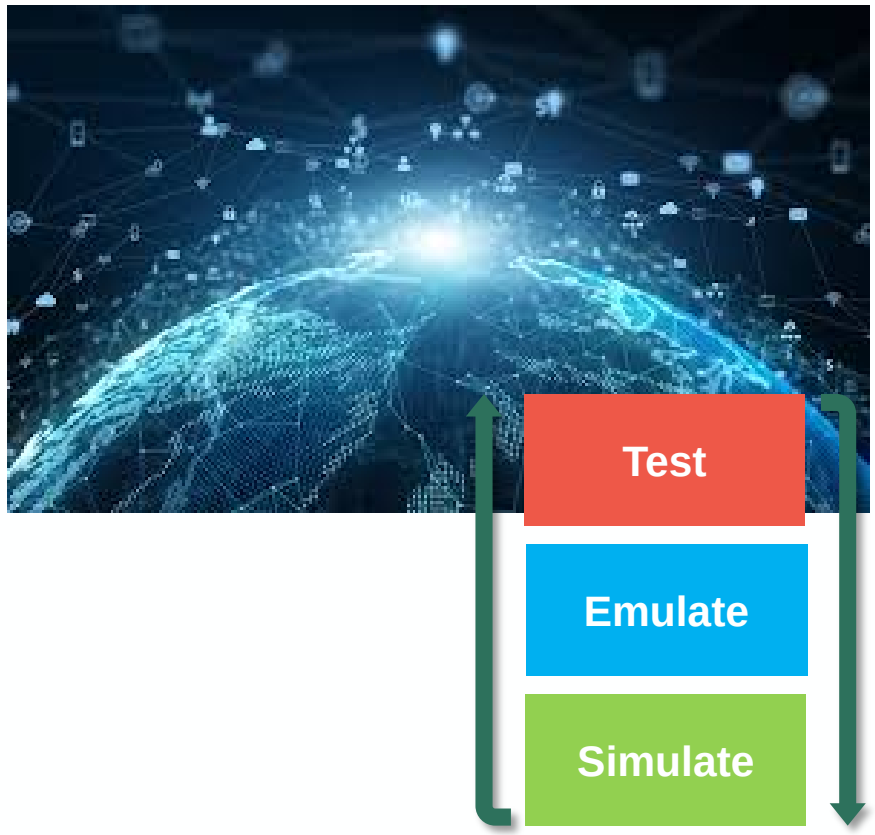
REALISTIC TRAINING ENVIRONMENT



CYBER RANGE – WHAT TO LOOK FOR (IV)

TEST BED FOR DIFFERENT DOMAINS & EXPERIMENTATIONS

MULTIPLE DOMAINS OF CAPABILITY



CYBER RANGE – WHAT TO LOOK FOR (V)

CURRICULUM & CATALOGUE

GAMIFICATION

Flexible

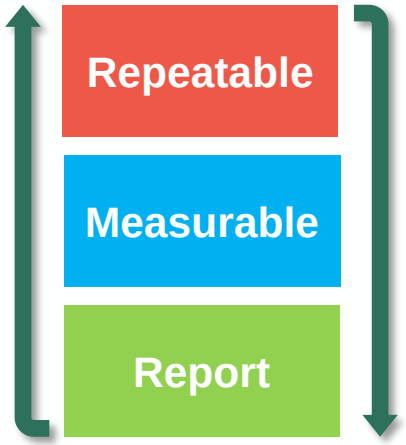
Fun

Effective

CYBER RANGE – WHAT TO LOOK FOR (VI)

REPORTING

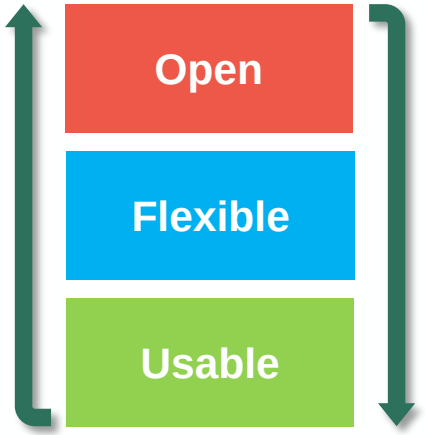
- Reporting & metrics tools.
- Allow range admin to assess performance & improvement over time.
- Internal reporting on effectiveness & retention for employees (based on real job) allows ROI to be calculated.
- Enable pinpoint strength & weaknesses & knowledge gaps.



CYBER RANGE – WHAT TO LOOK FOR (VII)

TOOLS-AGNOSTIC

COMPREHENSION & COMPETENCY FOR TRAINEES



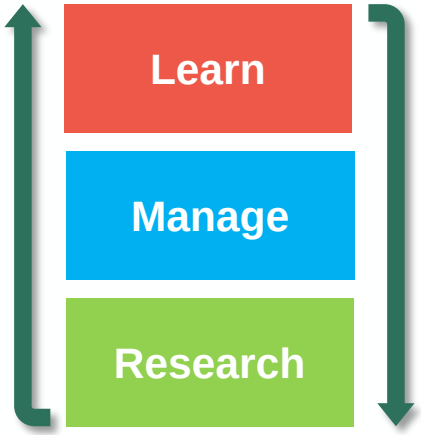
CYBER RANGE – WHAT TO LOOK FOR (IX)

REPLAY, REPRODUCIBLE & REPEATABLE VALUE

SIMPLE REPORTING / DASHBOARDS

CUSTOMIZABLE & SCALABLE

- One size does not fit all,
- Customizable to any environment, scalable and elastic



CYBER RANGE – WHAT TO LOOK FOR (X)

INTERNET CONNECTION IN SECURE MANNER

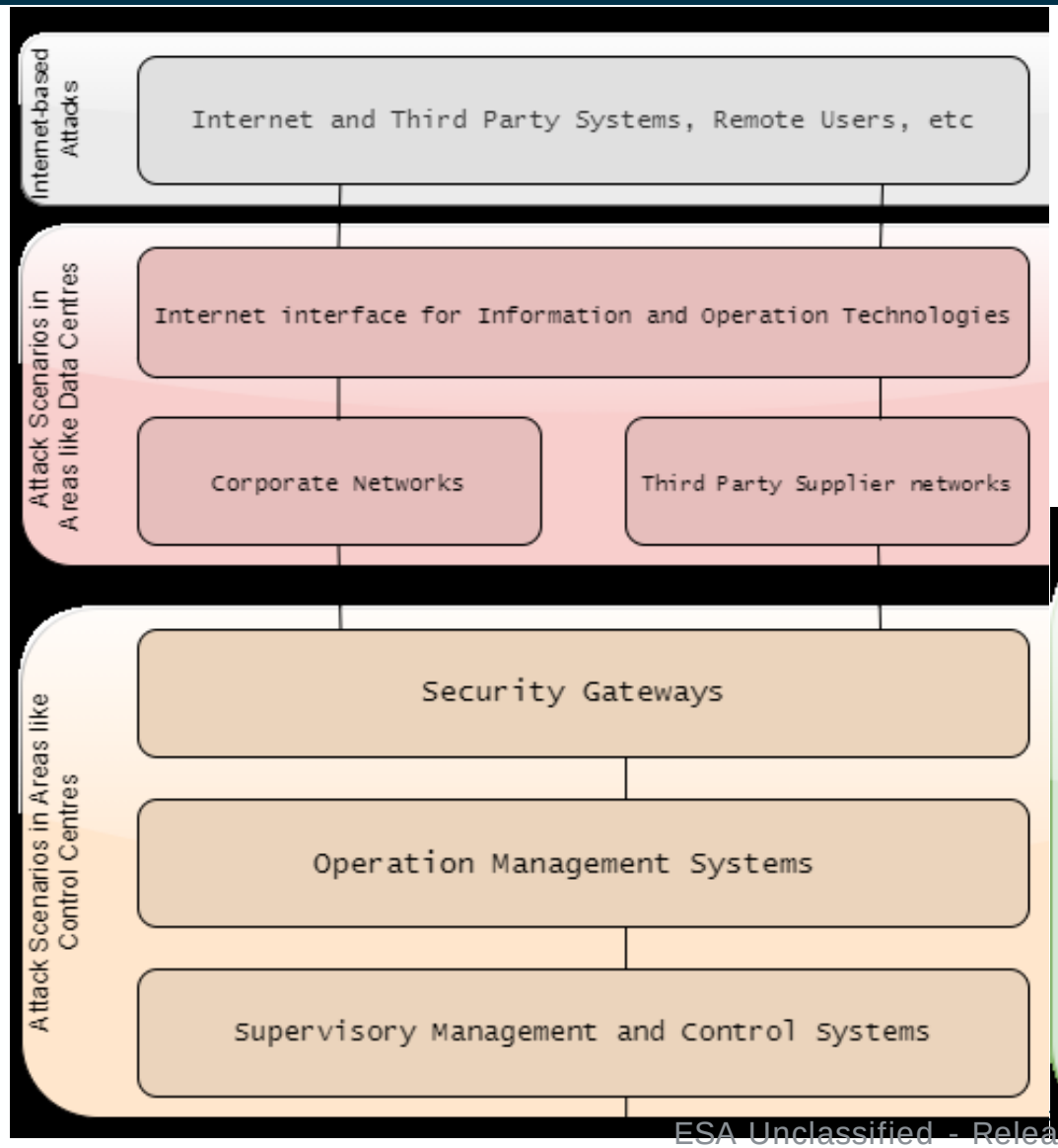
EASY TO SETUP & DEPLOY

SUPPORTS VARIETY OF CYBERSEC SKILLS

ABILITY TO AWARD CONTINUING PERSONNAL DEVELOPMENT (CPD) CREDITS

SUPPORT MULTIPLE TRAINING & EXPERIMENTATION USE CASES

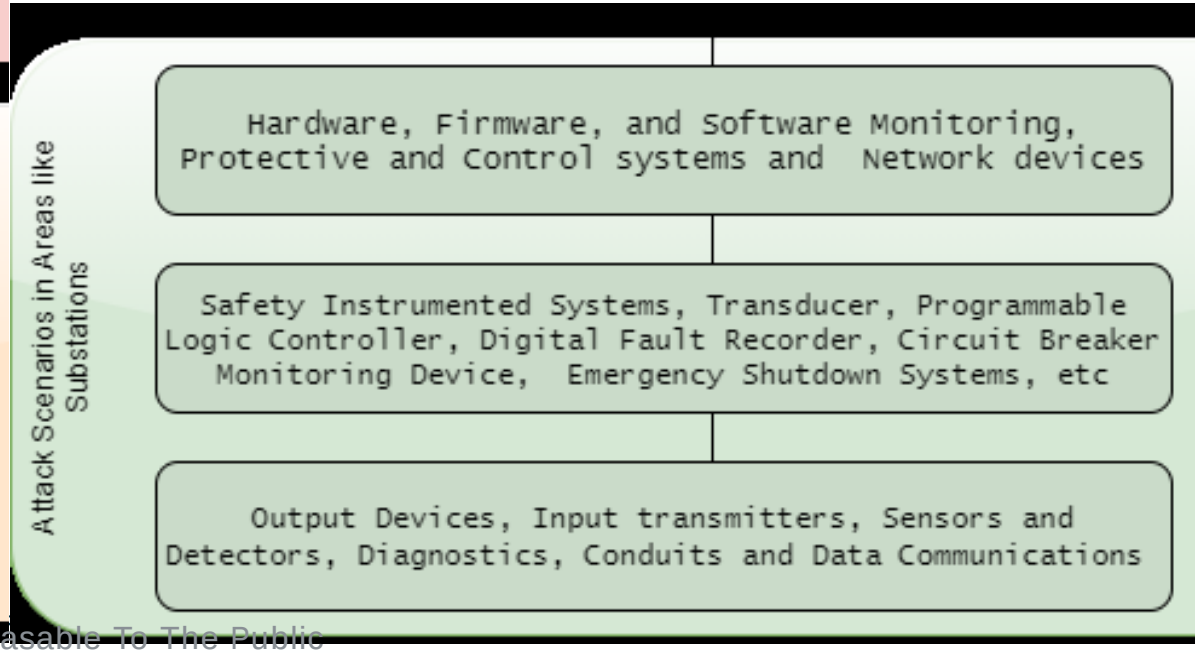
CYBER RANGE – SCENARIO EXAMPLES



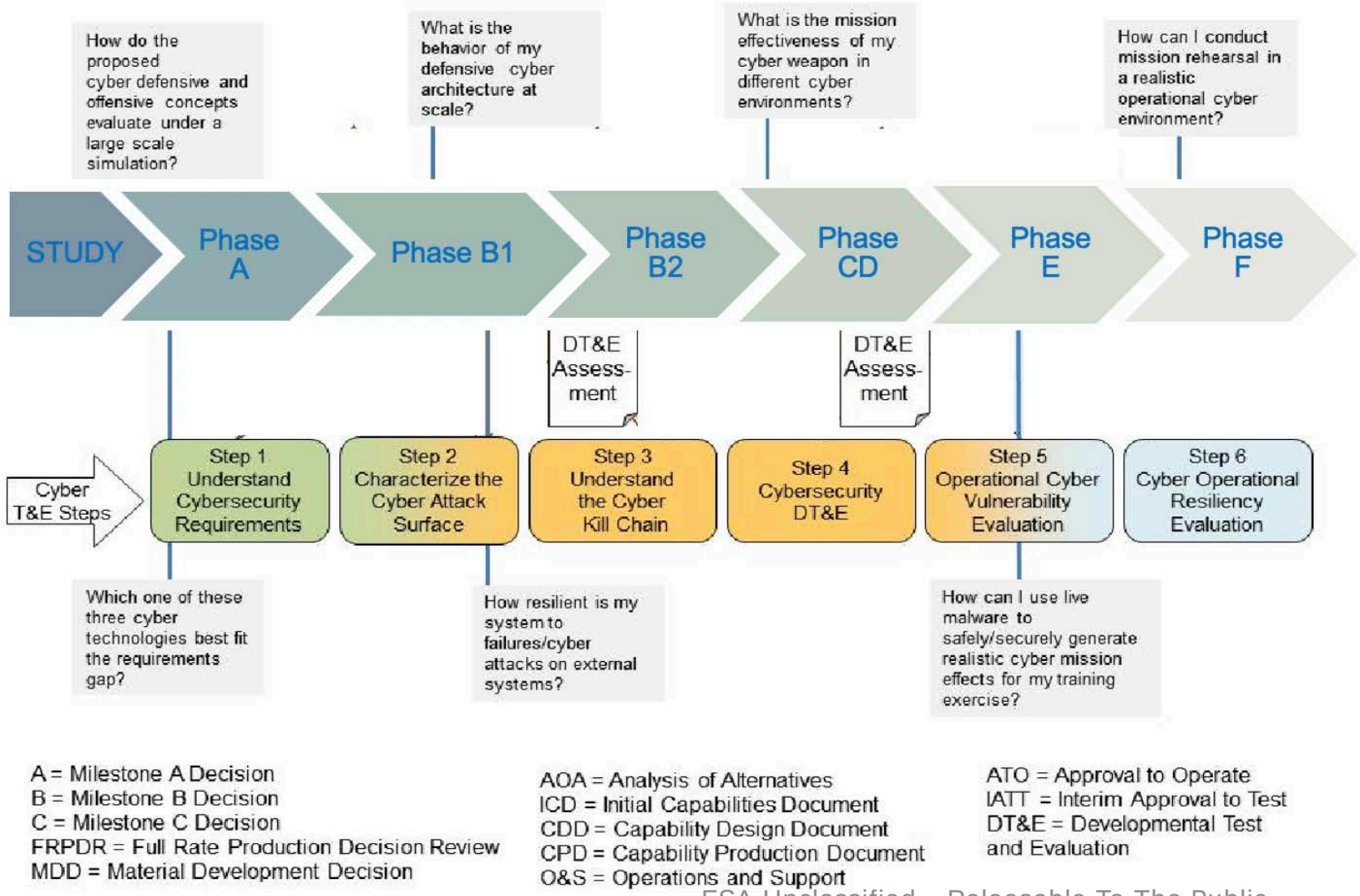
Example Scenario Types

- Components / Subsystems/ OT
- Networks & gateways
- Systems

Space, Ground, Portable, hardware in loop



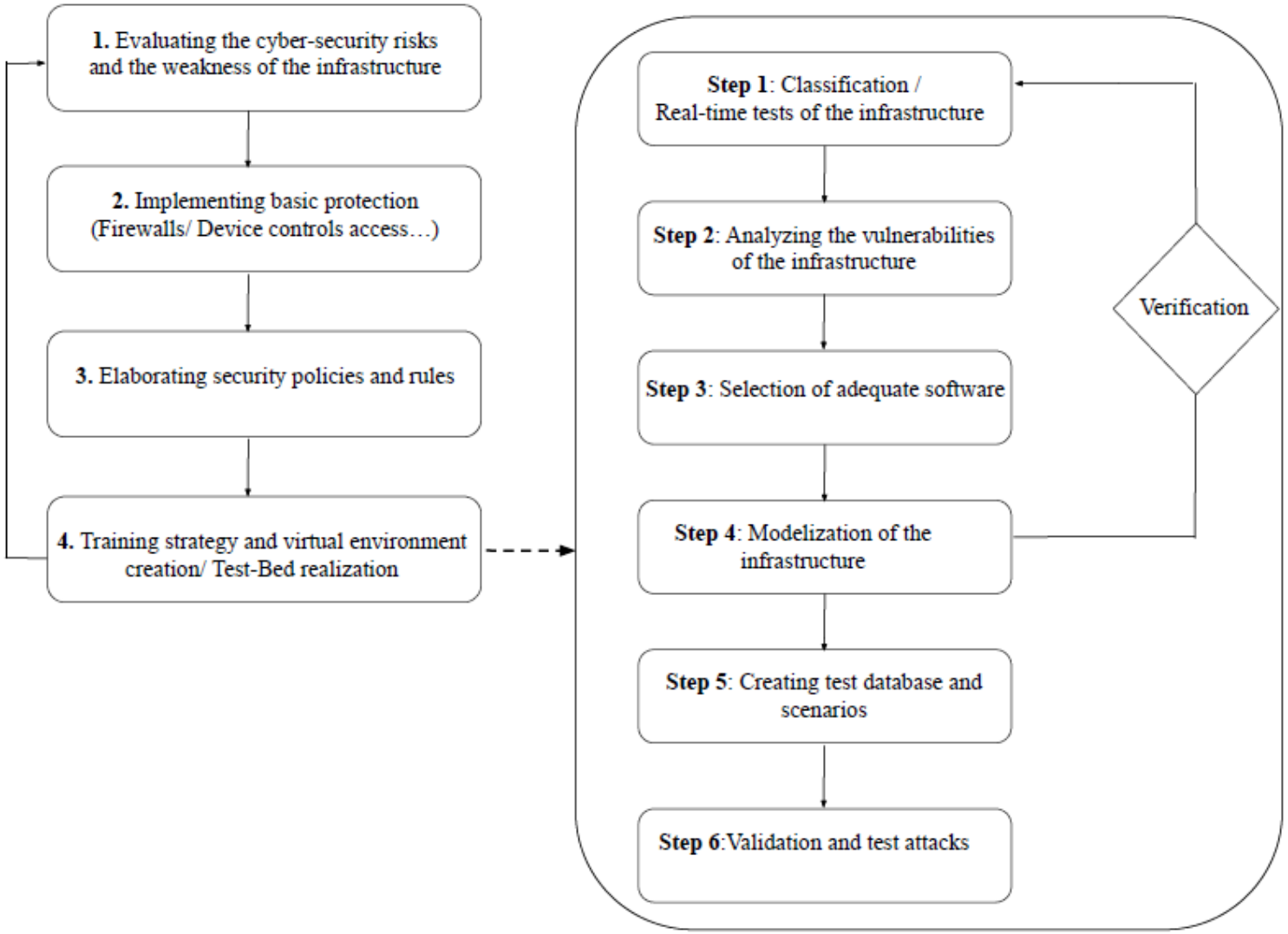
CYBER RANGE – EXAMPLE SDLC USAGE



USE IN SYSTEM LIFECYCLE

- Risk Assessment
- Threat evaluation
- Technology assessment
- Behaviour & vulnerability
- Training

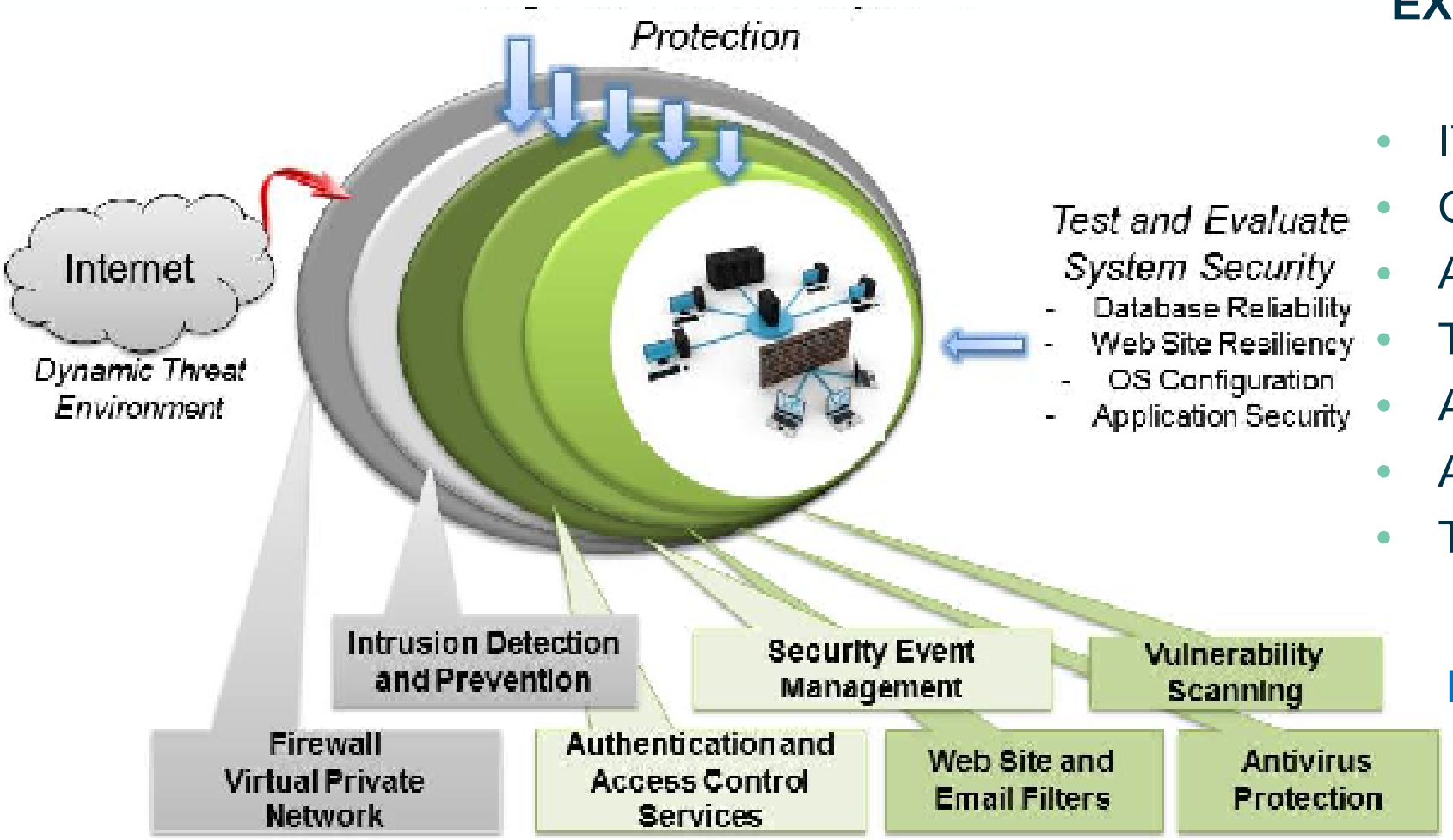
CYBER RANGE – EXAMPLE WORKFLOW



EXAMPLE FOR A CYBER RANGE / TEST BED

- Risk analysis
- Threat and vulnerability
- Environment model
- Potentially hardware in the loop
- System in the loop
- Control elaboration
- Training
- Testing
- Evaluation / assessment

CYBER RANGE – EXAMPLE NETWORK SCENARIO

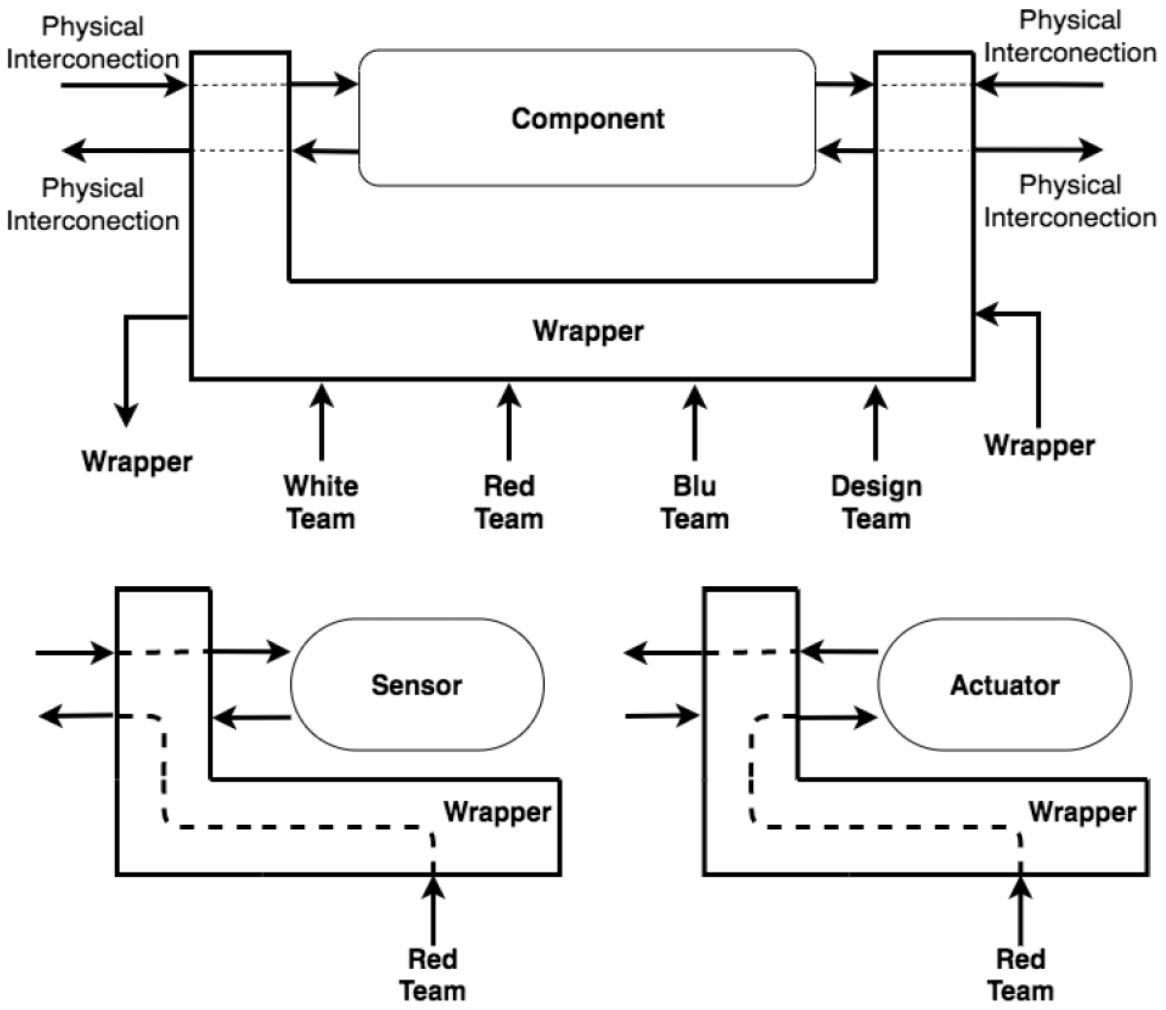


EXAMPLE TO SCOPE TESTING, EVALUATION

- IT network
- OS
- Apps and multilayer
- Tools, Tactics Procedures
- Assess Risk
- Assess & Identify Vulnerability
- Threats

New technologies, OT + Space, Zero-Trust models, Cloud / Virtual / Container

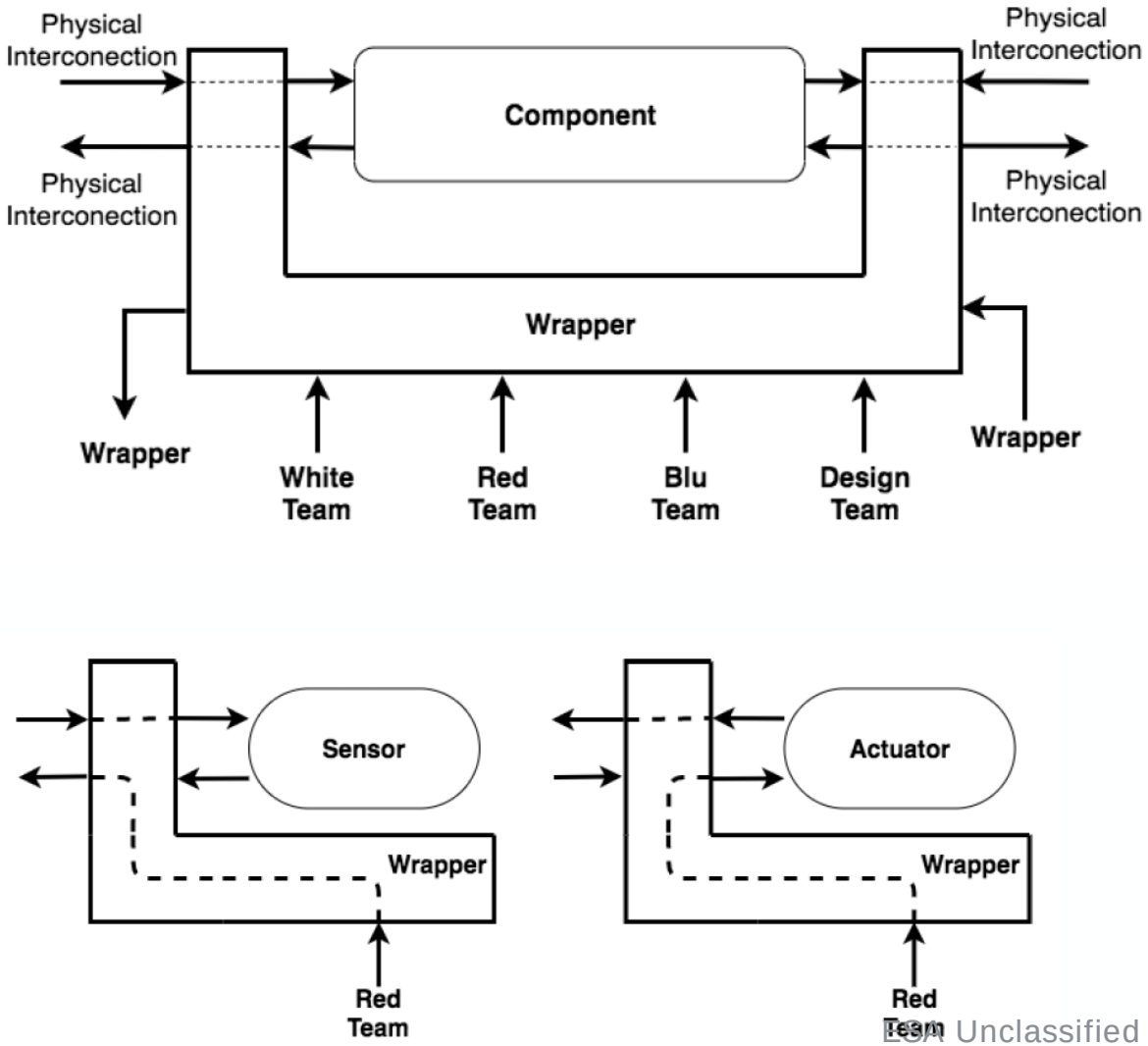
CYBER RANGE – EXAMPLE OT TYPE SUPPORT (I)



EXAMPLE USE CASE TO ENABLE TESTING / EVALUATION OF A COMPONENT

- Concept of wrappers around key components network / protocols
- Enabler to loosely couple the tools from emulators/simulators and hybrid / hardware in the loop tests
- Enabler for injection of scenarios/patterns/data to support external and internal flows:
  - Automated/scripted
  - Support to Red-team & scenario manager

CYBER RANGE – EXAMPLE OT TYPE SUPPORT (I)



EXAMPLE USE CASE TO ENABLE TESTING / EVALUATION OF A COMPONENT

Security Modes of use:

- Passive (to monitor/capture traffic/data flows properties)
- Vulnerability injection (control i/o)
- Vulnerability remediation (proxy to support blue team patches/investigations)
- Attack injection (control i/o) – allows attack (or defence) control without affecting real component
- Behaviour modification (control i/o to component) – allows emulate new components/protocols, solutions/hardware or software without affecting physical model
- Mock up – adaptability/elasticity to add new components (HW or SW) without rebuild system

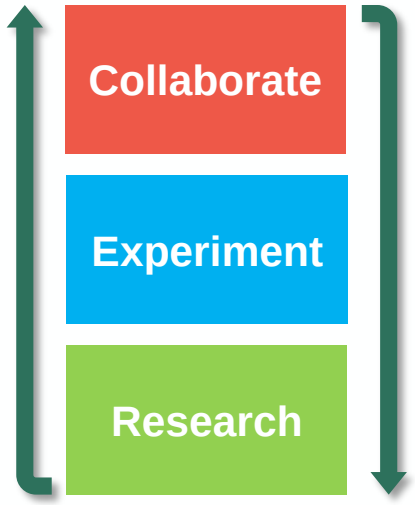
AGENDA

1. ESA in Security Context
2. What is a CoE ?
3. What is the ESA SCCoE ?
4. ESA Roadmap for the ESA SCCoE?
5. Getting onboard

ESA SECURITY CYBER CENTRE of EXCELLENCE (SCCoE)

ESA SECURITY CYBER CENTRE of EXCELLENCE

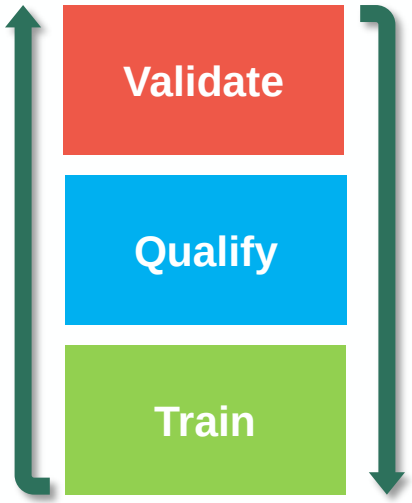
- Establish a **knowledge lead** for security of Space & IT Systems
- **Study, share, understand** & awareness about cyber issues
- **Train, test, exercise & develop** world class cyber-security services & procedures
- **Establish shared test-bed** to develop, integrate and test advanced cyber-security technologies
- Support **security evaluation, qualification & testing** with high capability toolset with Space focus
- **Collaborate** in development of incident handling/response measures & processes
- **Facilitate collaborative research & experimentation** for ESA, industry & partners



- **Help ESA to work in synergy & break the silo's**
- **Build an ESA strength in depth cyber resilience agency wide**

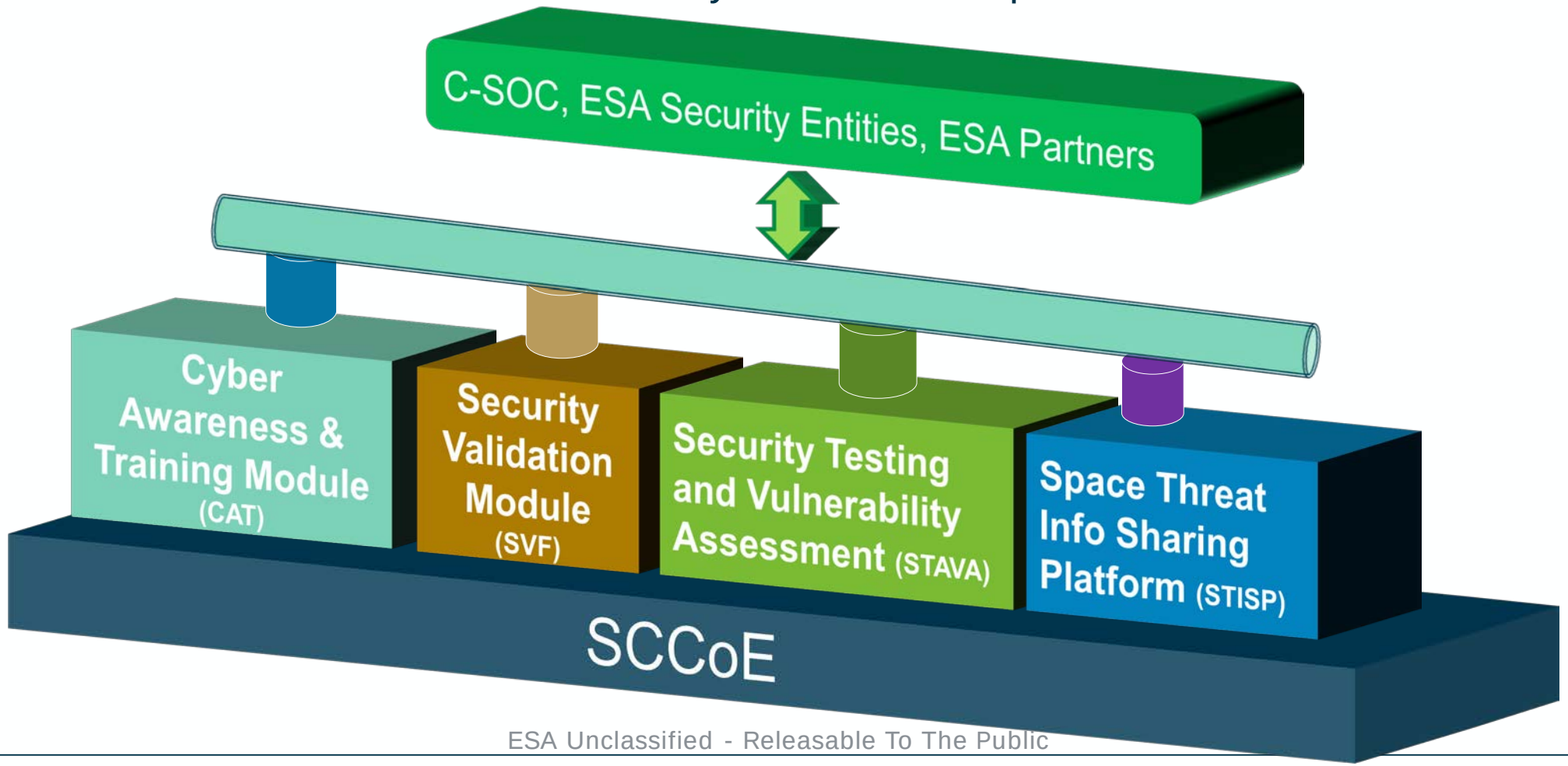
ESA Space Security Centre of Excellence
SCCoE Technical Objectives

- Training, Testing, Qualification from component to system, IT/OT & Space
- State of the art with ability to assess current & future technologies
- Dynamically scalable & elastic. Parts deployable/ pluggable to other systems.
- Easily useable and accessible by all users in all domains (service desk/catalogues/dashboards etc)
- Interfacing with internal (such as C-SOC) & external systems:
  1. cyber ranges
  2. projects
  3. tools (potentially digital twin/MBSE)
  4. and labs, CERT
  5. Exercise/conference collaborations (e.g. hackasat/defcon etc)



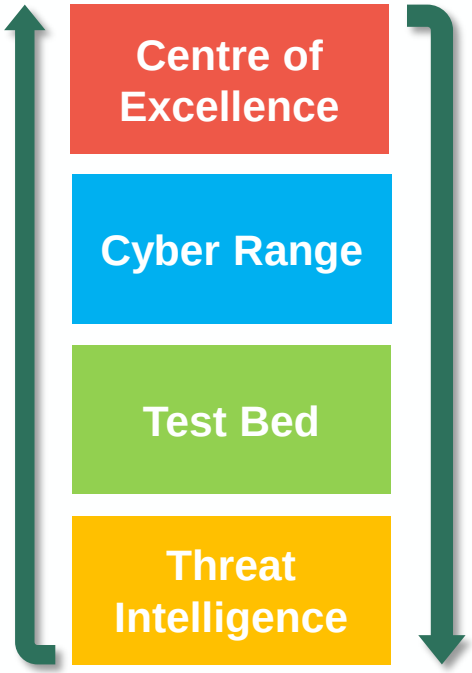
Synthetic SCCoE Modular Building Blocks

Security Cyber Centre of Excellence (SCCoE) aims to provide a unique capability in Europe in the frame of Space Cyber Security, in terms of training, test and validation services, and centralization of cyber services/expertise.



ESA SSCoE Summary of Features

The ESA SSCoE



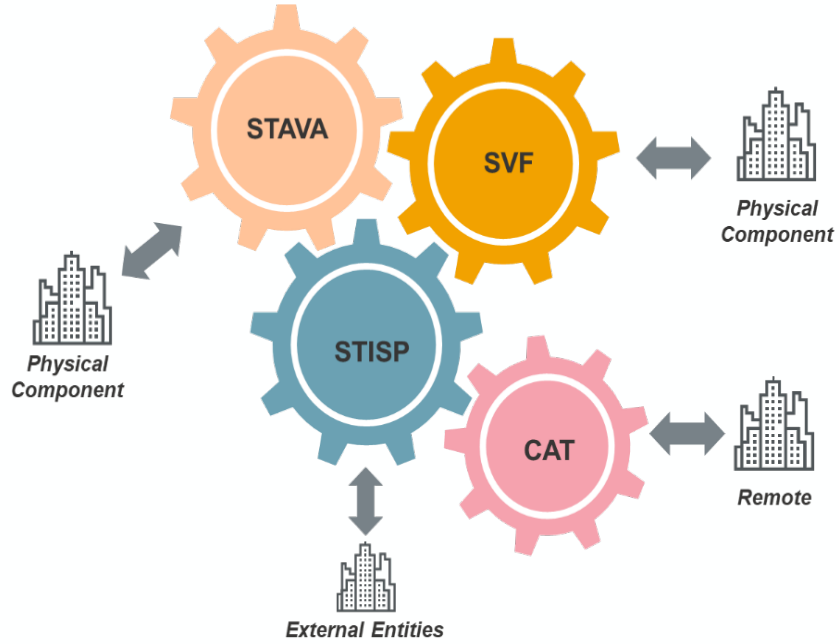
ESA SCCoE CORE KEY FEATURES (CAT)

Cyber Awareness and Training centre (CAT)

Training and methodologies capabilities for ESA staff, contractors, operators, engineers and managers on all cyber topics (cyber range)

Variety of delivery methods

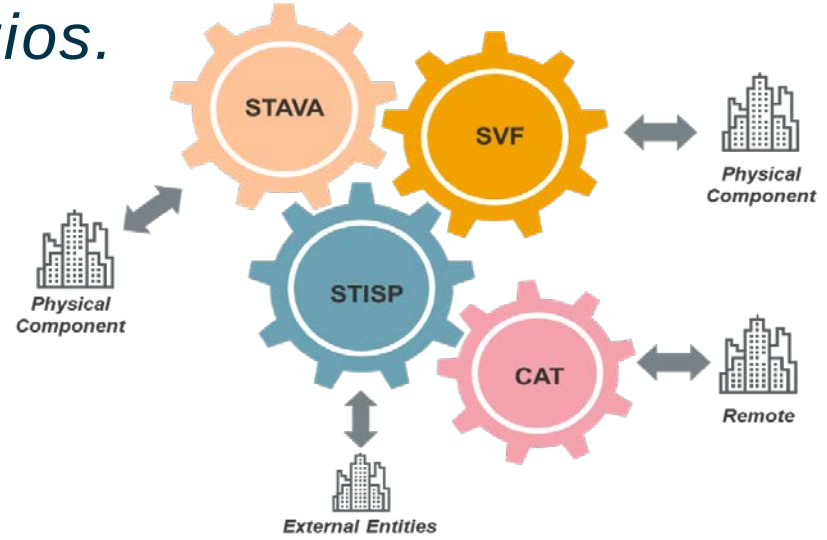
Basic & Advanced training packages



ESA SCCoE CORE KEY FEATURES (SVF)

SCCoE Security Validation Functionalities (SVF)

Emulation environment for step-by-step validation process for security procedures (e.g. SECOPS), mechanism, control or solution within simulated Cyber threat scenarios.



Security Space Programme emulation Scenario

Corporate, study, system, sub-system

Validate Security Procedures vs customised Security Scenarios

Interconnection with external components and subsystem

ESA SCCoE CORE KEY FEATURES (STAVA)

Security Test and Vulnerability Assessment (STAVA)

Testing & validation to assist in security certification and accreditation of current/new components, subsystems & systems.

Cyber security scenarios to validate/qualify current and new critical space and ground segment elements

- assess risk, vulnerabilities
- component to full system

Security tools and facilities with ESA IT, OT & 'Space' across System lifecycle

- assess adequacy and effectiveness and security measures for complex systems
- identification of security issues, deficiencies, risk, vulnerabilities

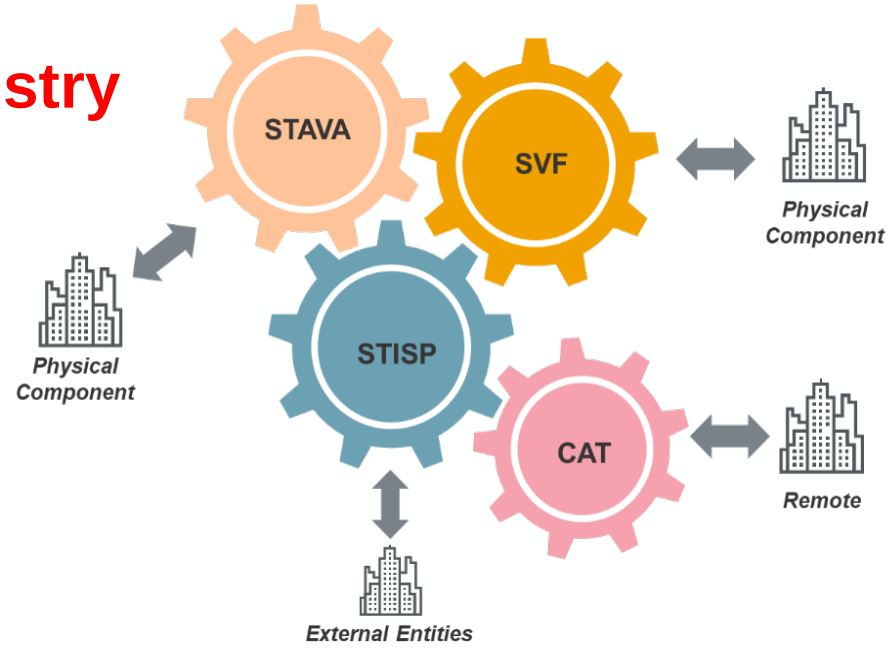
- Simulated, emulated, overlays & 'hybrid' scenarios with hardware in the loop
- Local, external and full test data generation
- Plug & play capabilities (e.g. api)
- Automation & Orchestration in user friendly manner

ESA SCCoE CORE KEY FEATURES (STISP)

Security Threat Intelligence Sharing Platform (STISP)

An ESA built space security threat intelligence and information sharing platform and portal to enable ESA members and partners to exchange cyber and space related threats and information in near real-time within a secure and controlled environment.

Enabler provided by ESA, but for ESA EU Space Industry Collaboration to protect space assets



ESA, partners & industry

Threat and vulnerability, intelligence & incidents sharing

Incident handling and report sharing facilities

Alerts (in normative reporting standards)

Reports and knowledgebase

- (documents, presentations, packages, training resources, whitepapers, …)

Threat Intelligence and Information Sharing Platform

Alerts
Standards
Knowledge

AGENDA

1. ESA in Security Context

2. What is a CoE ?

3. What is the ESA SCCoE ?

4. ESA Roadmap for the ESA SCCoE?

5. Getting onboard

AGENDA

1. ESA in Security Context
2. What is a CoE ?
3. What is the ESA SCCoE ?
4. ESA Roadmap for the ESA SCCoE?
5. Getting onboard

ESA Space Security Cyber Centre of Excellence

ESA Space Security Cyber Centre of Excellence

Cyber security test and Vulnerability Assessment

Independent security testing of space systems & products
Vulnerability analysis, penetration testing
Tools to assist system security qualification, risk, validation
Certification, Accreditation support - in line with different schemes

Cyber Awareness & Training

Train users, operators, engineers and managers on IT & Space Security

Extensive Curriculum
General awareness training
Expert (e.g. ISO, SRMP) training
Advanced security education
Security-by-design principles
Secure network implementation & configuration
Security incident management
Security forensics

01 Cyber Training

3 Cyber Security Test and Vulnerability

02 Cyber Threat Intelligence Sharing

Cyber security research, Threat Intelligence delivery

Collaboration tools for ESA & partners
Threat Intelligence, analysis and sharing
Security risk assessment tools
Secure solution research and experimentation
Vulnerability and malware research

Cyber security exercise hosting & participation

Cyber-Sim exercise hosting
Exercise planning and coordination

Operations procedure development validation and experimentation
New product experimentation, testing

ESA SCCoE – who & why

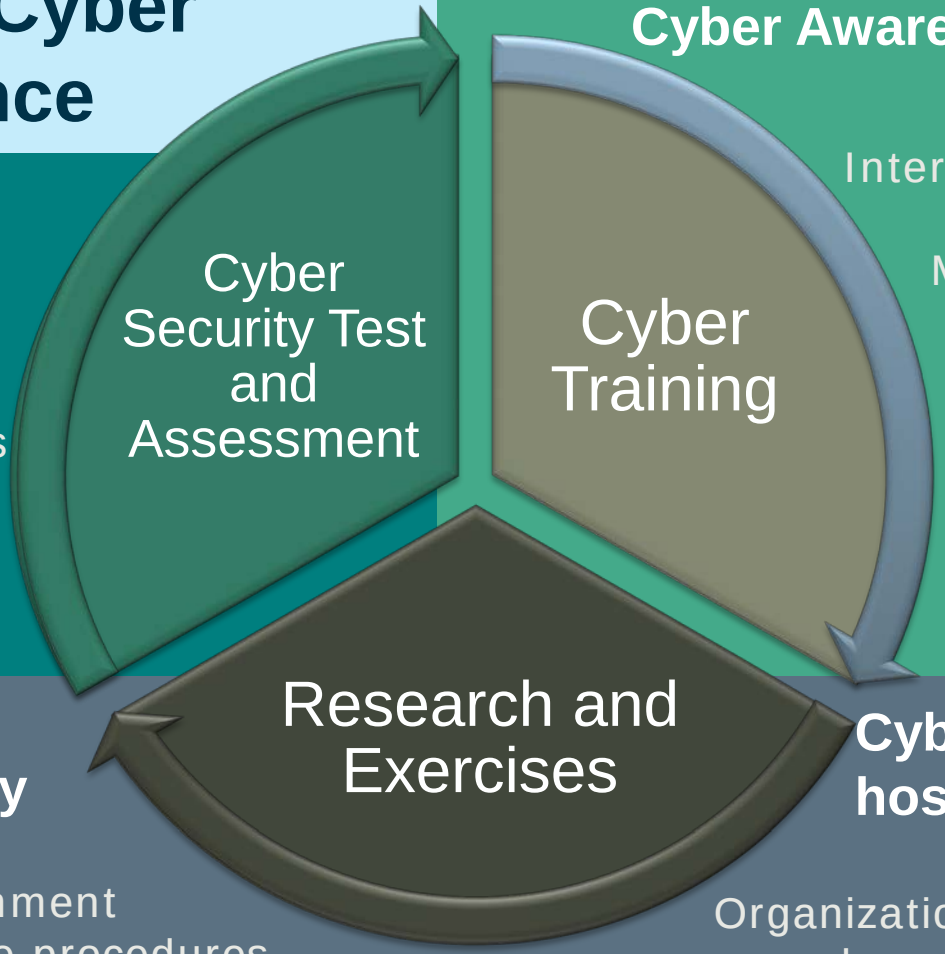
ESA Space Security Cyber Centre of Excellence

Cyber security test and Vulnerability Assessment

Projects – reduce new activities and access expertise to be secure
Developers – access tools & resources
Operators – assess risk and updates
Experts – access tools & resources
Evaluators – enable conformity

Cyber Awareness & Training

Internal Users – increase awareness & expertise
Managers – understand needs & tools
Partners – access experience
Expert training and hands-on in controlled environment



Cyber security research, Threat Intelligence delivery

Developers – try in controlled environment
Operators – access expertise, validate procedures
Professional – experiment, collaborate – assess threat landscape

Cyber security exercise hosting & participation

Organization – raise profile, credibility and expertise
Experts & Operators – build network and knowledge
Industry – access expertise and build competence

QUESTION/DISCUSSION