The ESA Cyber Range in Redu:
Why it is important for ESA, EDA and all of us

Stefano Zatti
Head of ESA Security Office

14/05/2018

What is a Training Range?

What is a Cyber Range?

A **cyber** range is a ***virtual*** environment that is used for cyber warfare training and cyber technology development.

It provides tools that help strengthen the stability, security and performance of cyber infrastructures and IT systems used by government and military agencies.

Goals of the Project

To develop a training and simulation platform facility to provide training and testing and develop knowledge in Awareness, Detection, Investigation, Response and Forensics to counter cyber-attacks specific to the Space world.

The system is used and accessed via an existing training class-room in ESA Redu.

The benefits of simulation

- Real experimentation on isolated virtual infrastructure (sandboxing)
- Training the teams against known attack scenarios
- Increasing the staff detection and response skills
- Raising awareness about information system security
- Discovering, practicing attacks and highlighting weaknesses on a clone of a space control system
- Prototyping, testing and evaluating new architectures
- Validating new components or configuration before definitive integration
- Simulating a specific user population on a particular IT infrastructure component
- Developing new ways to increase the protection against attacks.

Architecture of the Space Cyber Range

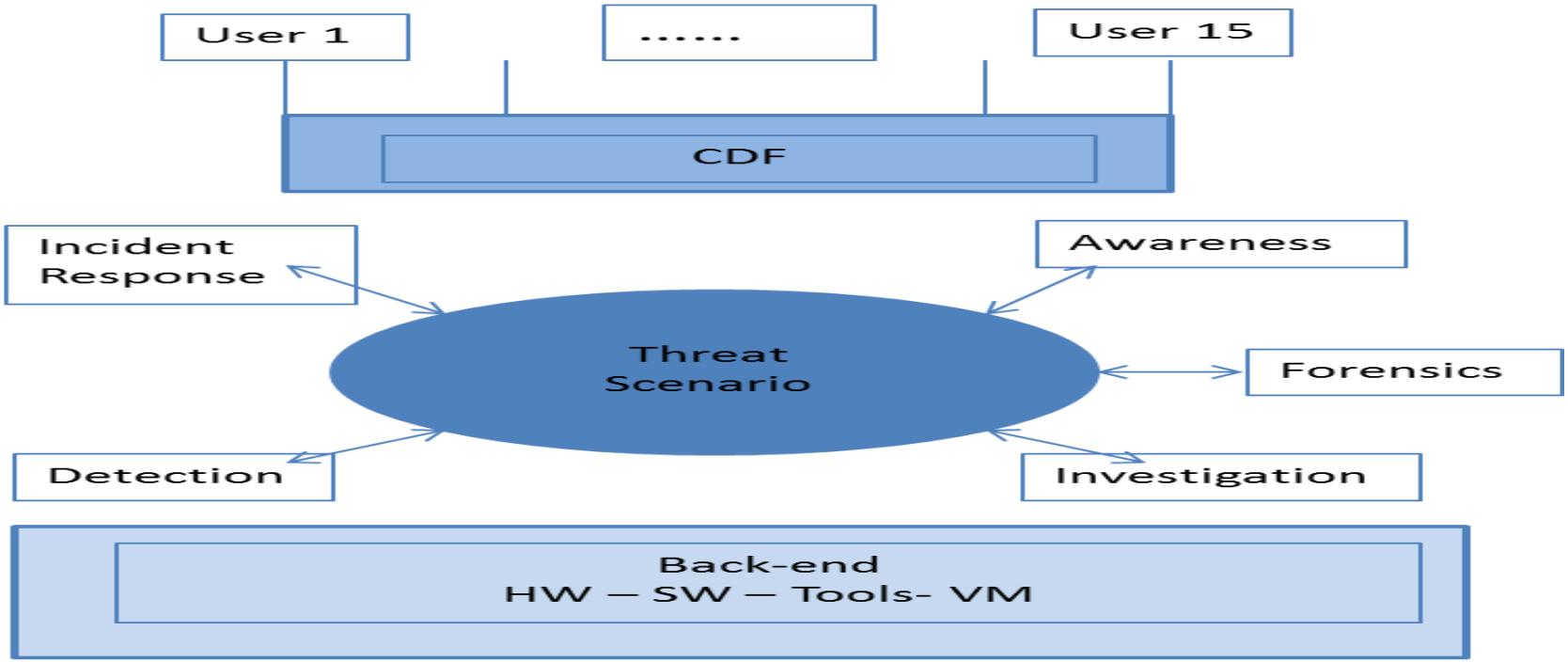

Figure 1: Cyber security training range set-up

Training and demonstration scenarios

The scenarios shall cover, for each mission category, the different phases of a space mission, namely:

- Pre-Launch
- Launch
- LEOP
- IOT
- Operations

subject to different kinds of threats that require customized training in the related space mission elements as:

- Space segment
- Data segment
- Ground segment

Training exercises

The current contractual activity for the cyber range have foreseen the deployment of the back-office infrastructure and the demonstration of it capabilities in three training sessions, that took place in 2017 and saw a very positive reaction by the audience:

• Awareness:	HOCAT	2 days
• Incident response:	CYFRT	3 days
• Forensics analysis:	AIRFIT	5 days

Exploitation Phase

The exploitation phase, after 2017, will exploit the system to perform activities like:

- Training and awareness on new scenarios or space mission categories
- Technology research, development, experimentation and test
- Collaborative information sharing and analysis
- Operations procedure development and experimentation
- Legal, Policy and Capability requirements research

Exploitation Phase

Involvement of new partners: the constituency broadens

- **ESA and its mission managers**, to instruct their staff and provide additional, more tailored scenarios addressing their main experiences and their security concerns;
- **Other relevant space agencies (CNES, DLR) and other peer organizations (EDA, defense ministries of Member States, cyber authorities)** to enrich the contents and suggest additional scenarios according to their views and their needs, as well as addressing their fears;
- **Industrial partners,** who beyond contributing to the contents of the sessions, could be interested in operating their own programs at the facility, as developed later.
- **Academic partners** representing the educational side, that will want to additionally contribute to the training curricula and suggest novel research paths.

Conclusions

After the initial phase until end of 2017, it is foreseen that the cyber range will be able to live its own life, by ensuring continuity and funding with the mechanism outlined above.

The challenge to keep it alive and growing will be to find new users and interested parties to make use of the facility to create and validate new scenarios and training curricula.