CYBERRANGE LUXEMBOURG

Cyberday.lu

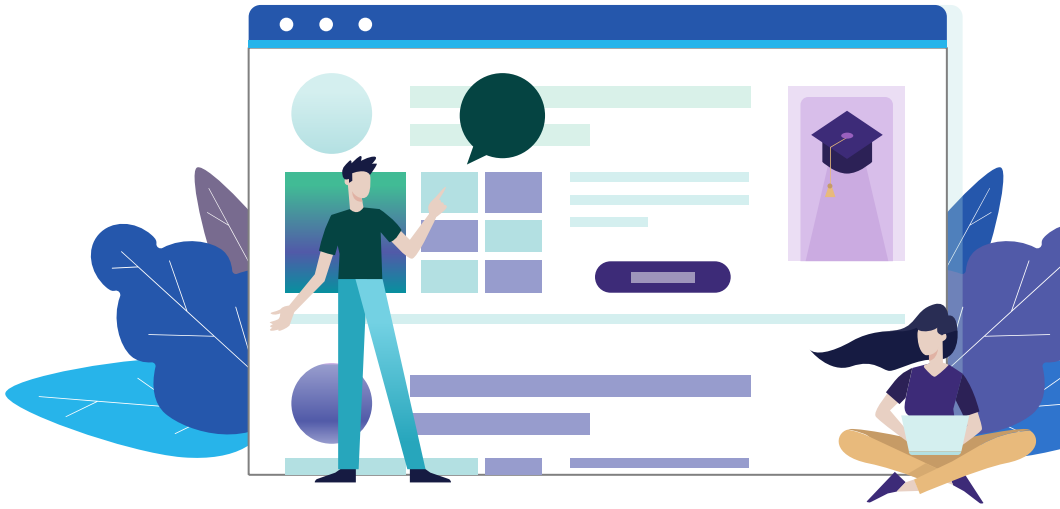
12/10/2023

cyberrange@mae.etat.lu

What is a Cyber Range?

What is a Cyber Range?

- A controlled, interactive simulation environment.
- Contains the tools to define learning scenarios or test beds by creating digital twins of real live environments
- A save place to learn for organizations and individuals providing them feedback on their skills and helping to identify gaps



What is a Cyber Range?

Why should one invest into a Cyber Range?

Cyber risks have evolved and have become a main **area of concern**

- **Strong resilience** to cyber-attacks is **required**
- **Need for developing and maintaining the level of knowledge and skills-set** of cyber security practitioners

Thus the need **for setting up of an advanced cyber-security training center** in the form of a **Cyber Range**

Key benefits expected from a Cyber Range

- Improve personnel cyber posture
- Keep cyber security professionals skilled and ready
- Assess procedures and technologies in real scenarios
- Facilitate incident response and crisis management
- Develop team spirit, collaboration and communication
- Facilitate international cyber security cooperation
- Support for academic classes and academic research
- Test the real impact of security controls

Usage Scenarios (1/6)

Live fire exercises and threat hunting

- Objectives:
  - Detection and prevention of attacks;
  - Network monitoring;
  - Situational awareness and control;
  - Handling cyber incidents;
  - Teamwork: delegation, dividing and assigning roles, leadership.
- Accommodates a variety of scenarios including physical incidents causing cyber consequences, ransomware, compromise of data centres, DDoS attacks, insider threat, malware outbreak in SCADA/ICS systems, web defacement etc.
- In a typical scenario, the exercise unfolds over two days in 4 escalating phases. This allows effective feedback and learning experience.
- A lightweight variation are threat hunting exercises which allow a guided approach for less mature teams

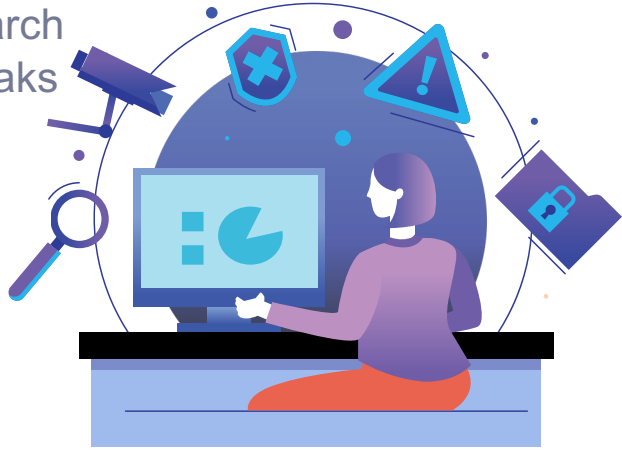
Usage Scenarios (2/6)

Strategic Decision Making

Objective: allow political leaders, high-ranking officials and advisors, and company executives to understand modern cyber threat landscape and enable them to deliver effective crisis management processes

- Play out a fictional cyber crisis by taking concrete crisis management decisions and exploring the (in)formal frameworks that govern decision-making processes - either independently for purely management training events or in combination with the cyber range to create a holistic technical-strategic exercise

- Scenarios may include different types of organizations (e.g. businesses, educational or research organizations or nations) and simulate threats such as ransomware, DDOS attacks or data leaks



Usage Scenarios (3/6)

Capture the flag (CTF)

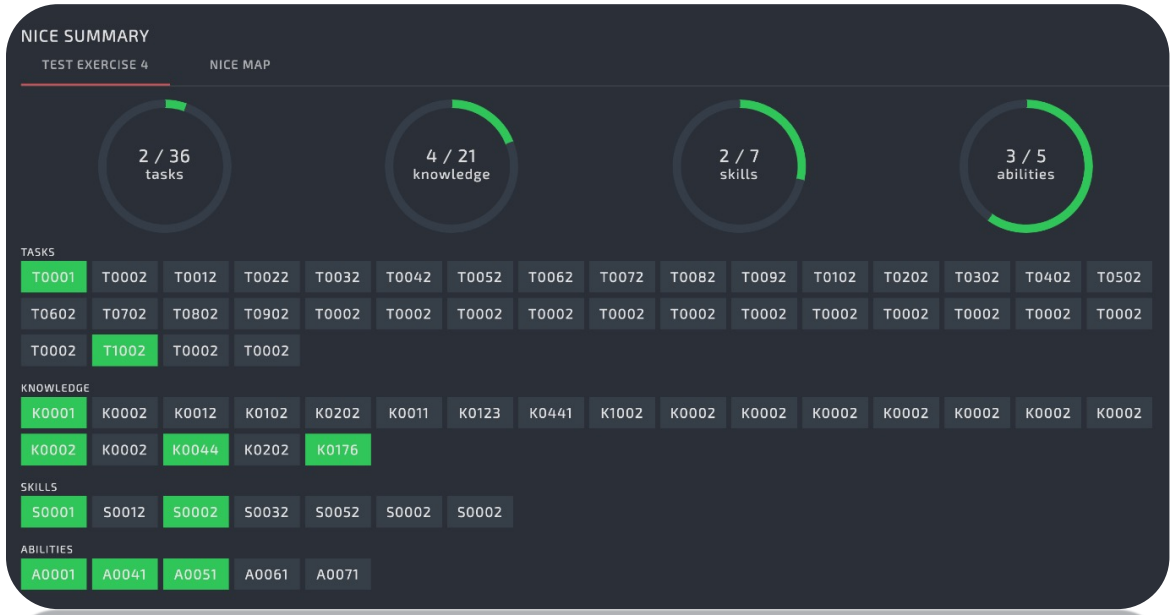
Allows flexibility in setting the conditions and content of an event:

- Participant Structure – Individual or teams.
- Type of Tasks – Theoretical and practical; for the latter, GameNets or virtualized networks in a cyber range are used to complement the environment.
- Training Flow – Fixed flow, where tasks are “locked” into a chain of challenges, or loose flow, where participants are free to choose and fulfil tasks
  at their own preferred order.
- Limits and Timing – No restrictions; participants can be put under heightened pressure by various means such as time limits and penalties for task failure.
- Scoring and Elements of Competition – Participant progress is scored and maintained; for competitive events, a live scoreboard is included.
- .

Usage Scenarios (4/6)

Skill Testing and hiring

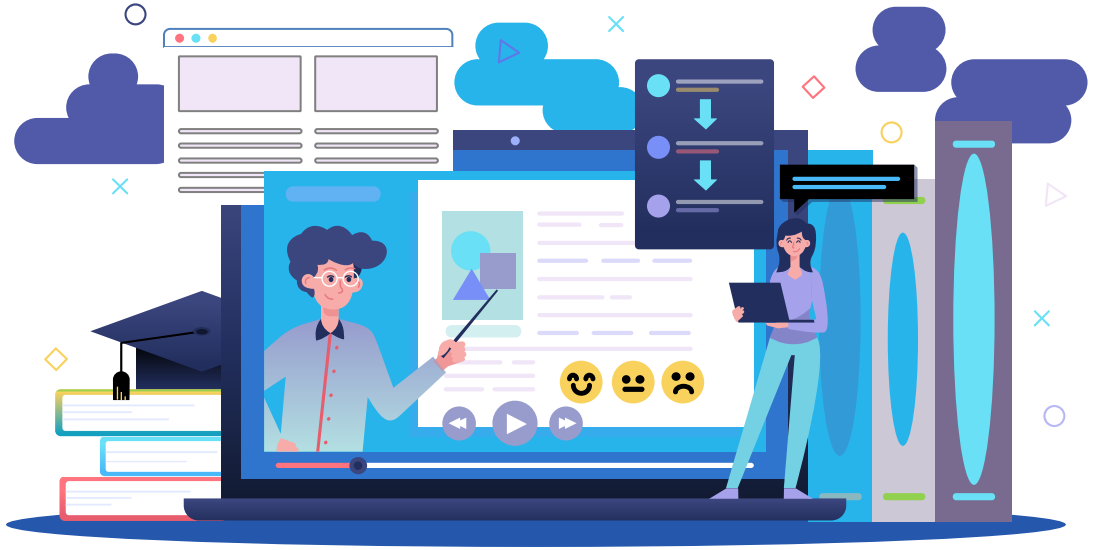
- Find out strengths and areas for improvement
- Option to monitors a users progress.



Usage Scenarios (5/6)

Classroom Training

Use a build in or independent LMS to provide information to the trainees
Easily create multiple, independent instances of training environments



Usage Scenarios (6/6)

Security Testing

- Build your testbed based on your own VM templates or use the preconfigured ones.
- Use traffic generators to get reliable, reproduceable and comparable results.
- Scan for vulnerabilities
- Apply pen tests.

The Luxembourg Cyber Range

CYBERRANGE
LUXEMBOURG

Local and secure

Hosted in a local datacenter on NATO grounds fulfilling high security standards.

Usable by eligible partners

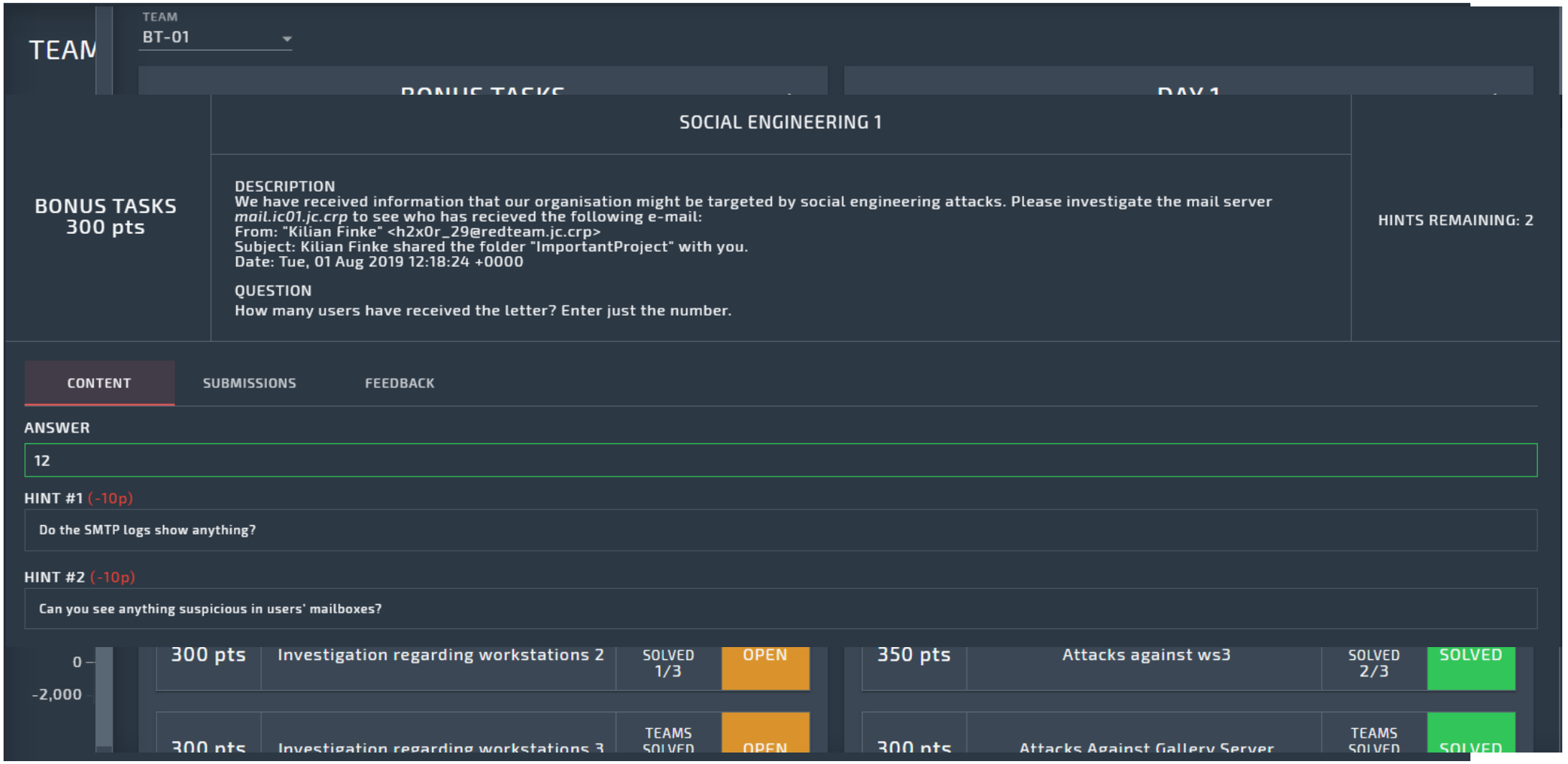
Not an offering for everyone but selected non-commercial partners (no competing with the offerings by commercial suppliers)

- LUX authorities (GOVCERT, MILCERT,…);
- LUX cybersecurity actors (CIRCL,…);
- **Education and Research (BTS Cybersecurity, Foundation RESTENA,..);**
- LUX critical infrastructure operators;
- LUX Partners (EU Member States, NATO Allies);
- NATO agencies & COE (NSPA, CCDCOE);
- EU Agencies (EDA - Cyber Range Federation project).
- Humanitarian organizations

Cost effective

Eligible partners get free access to the Luxembourg Cyber Range and assistance with their trainings (including the possibility to train their own trainers).

Cyber Range in Action



Want to feel the heat?

LOCKED SHIELDS

DO YOU HAVE ANY QUESTIONS?

CYBERRANGE LUXEMBOURG

Thank You

GET IN TOUCH

cyberrange@mae.etat.lu