Justine Ramelot, Research assistant
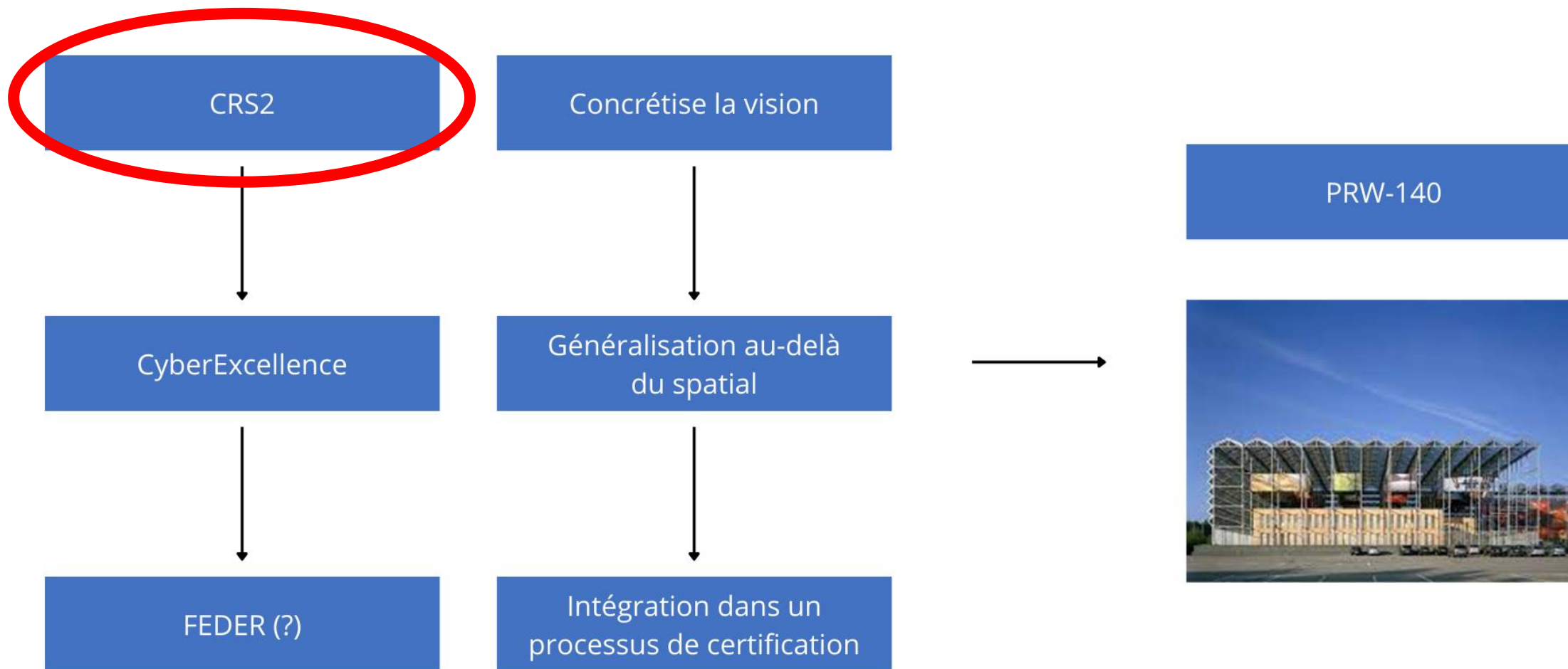- justine.ramelot@uclouvain.be

Cyber Range Scenarios (CRS2)
- Methodology for updating the virtualized infrastructures of the Cyber Ranges
- High-level fundamental research on a contextualized engine for the generation of flexible and adaptive scenarios on which the team trains to defend and/or attack

Involved in **CyberExcellence, WP5**: Laboratoires d'expérimentation, de validation, et d'entraînement

Focus on **Task 0**: Consideration of user needs for impactful applied research: specifically, conduct studies with users of the current system to identify their training and education needs

Placement within CyberWal

CRS2

Concrétise la vision

PRW-140

CyberExcellence

Généralisation au-delà du spatial

FEDER (?)

Intégration dans un processus de certification

Objective & expected outcome

- **Cyber Range**: a real-world simulation platform that allows security teams to train (attack and defense), develop their expertise, and manage their human resources planning

- **Objective**: generate the most realistic and appropriate training scenarios possible by specifying the components to be trained on, their interactions and the team's profile

- **Expected outcome**: deliver a new generic engine for the configuration and coaching of Cyber Range users

Materials and tools used

- **Prospect Day**
  - Cybersecurity Awareness training material
  - Live demos of CITEF (Cyber-security Integration, Test and Evaluation Framework) and CIRP (Control Incident Response Platform)

- **Compliance with UI guidelines**
  - Demo recordings and Shneiderman & Leavitt (2006)
  - Survey research to complete the guideline analysis

- **Formulation & Test-and-refine of (re)design ideas**
  - Low fidelity prototype (sketch) and reporting

Partners