



ATHENA Instructions

Instruction for trainings modules – supporting document

Webinar information

Organised by	Erik Akkermans
Date	August 2026
Target audience	OT leader, OT operator, Security advisor



Instruction

OBJECTIVE / GOAL

Instructions for supporting the ATHENA training modules

Technical instructions:

- Wi-Fi connection is required for the VR set (choice: hotspot, modem VR set, external wifi access) to be able to log in for sharing the results of VR training module to the LMS platform.
 - The demo can always be given without Wi-Fi connection
-

ATHENA WEBSITE

Website: <https://athena-digitalwater.eu/>

Link: [Athena | Strengthening Cybersecurity in Europe's Water Sector](#)

Selection: Proceed to Athena training

REGISTRATION

Login: <E-mail address>

Password: <Password>

You will also have to fill in this password in the VR-headset.

You can change the language (default German) at settings.

TRAINING MODULES

- Basic module: E-learning: Cyber Security in the water sector – *General knowledge*
General cyber security training based on three cases (at the lock, at a water treatment company and at a construction site). You are looking through the eyes of a hacker.

Duration: Approximately 30 minutes.

- Scenario 1: Prevention: VR training about Cyber Security - *Risk Awareness*
You look for cyber security vulnerabilities in a control room.
Tip: Search for an empty room of about three square meters where you can do this module standing or sitting. By pointing the joystick to the floor, you can 'jump' (hyperloop) to the desired position in the room (this way you must walk as little as possible).

Duration: Approximately 20 minutes.



- Scenario 2: VR training about Cyber Security - *Detection*
In a drinking water facility something unexpected happens during your shift. Investigate what is going on. Try to find the relationship with what if something like this happens at your location. Does everything work properly technically, which checks do you want to perform, what actions do you take and which people do you need to do so? Consult the facility manager (Peter) regularly to see if you have found all events.

Tip: Do this training sitting on a chair. Make sure you position the headset correctly on your head so that the subtitles aren't blurry.

Duration: Approximately 15 minutes.

- Scenario 3: VR training about Cyber Security - *Mitigation*
The participant takes the role of an OT leader who is nominated crisis manager during a large-scale cyber attack on the water infrastructure. On a Friday afternoon, the SCADA screens of the control room suddenly turn black and alerts are triggered. Calls from the general manager and the IT manager confirm that a certified account has been compromised and that the organisation is facing a proven cyber attack. A crisis situation is declared and the participant has to coordinate the response.

Throughout the exercise the participant communicates by phone with the general manager, the IT manager, the maintenance manager, the HR manager and the control room operator. The participant assesses the severity of the attack with a cyber severity matrix, which is filled in twice as the situation evolves, evaluates the quality and the coherence of the incoming information on an information quality board, resolves contradictions between field data and SCADA data, manages staff under time pressure, and finally selects the SCADA mitigation strategy: an immediate reboot of the main SCADA, or the activation of the backup SCADA site before rebooting the main system in secured conditions.

The scenario ends with a debriefing in which the key decisions of the participant are reviewed and scored, supported by the virtual assistant Leonard. The scenario trains situation assessment, information management, decision making, prioritisation and time management during the mitigation phase of a cyber attack.

Tip: Do this training sitting on a chair. Slide your chair back slightly to get a better view of the screens.

Duration: Approximately 30 minutes.





**Co-funded by
the European Union**

"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them."



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

The project funded under Grant Agreement No. 101127970 is supported by the European Cybersecurity Competence Centre

