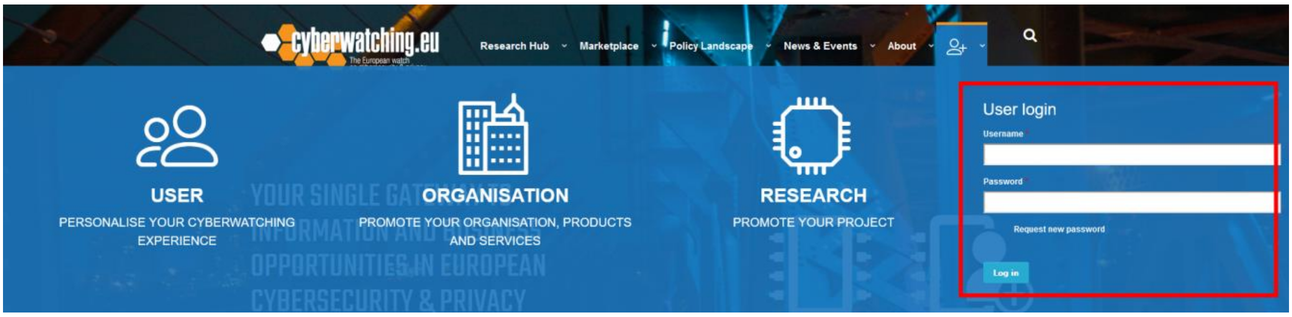
cyberwatching.eu
The European watch
on cybersecurity & privacy

HOW TO ADD YOUR PROJECT ON THE RADAR

Step 1 - Login to Cyberwatching.eu



cyberwatching.eu
Research Hub
Marketplace
Policy Landscape
News & Events
About
USER
PERSONALISE YOUR CYBERWATCHING EXPERIENCE
ORGANISATION
PROMOTE YOUR ORGANISATION, PRODUCTS AND SERVICES
RESEARCH
PROMOTE YOUR PROJECT
YOUR SINGLE GATEWAY TO INFORMATION AND BUSINESS OPPORTUNITIES IN EUROPEAN CYBERSECURITY & PRIVACY

User login

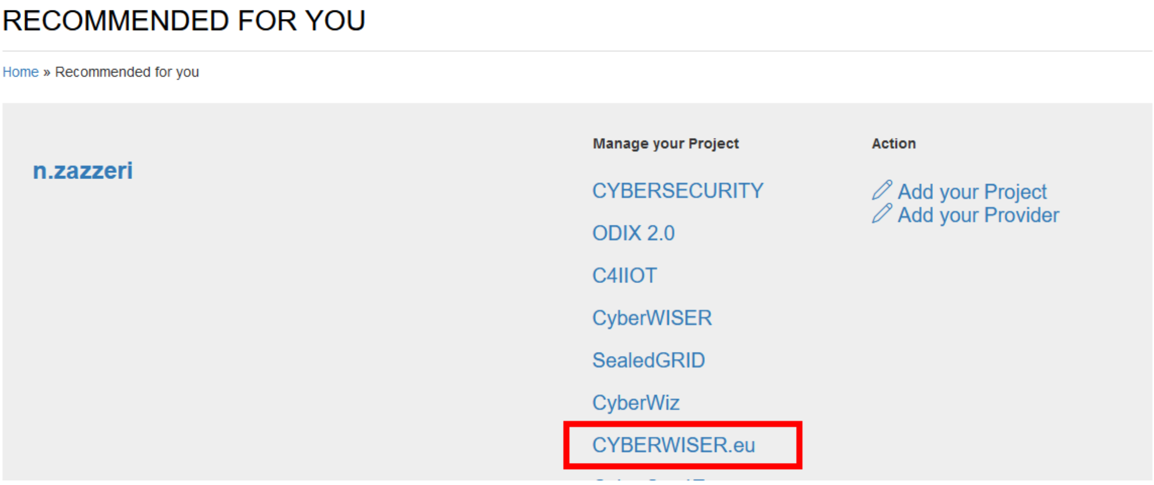
Username

Password

Request new password

Log in

Step 2 – Select the project you are managing



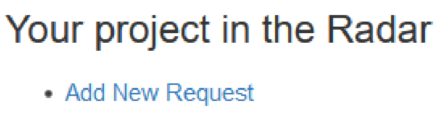
RECOMMENDED FOR YOU

Home » Recommended for you

n.zazzeri

Manage your Project	Action
CYBERSECURITY	Add your Project Add your Provider
ODIX 2.0	
C4IIOT	
CyberWISER	
SealedGRID	
CyberWiz	
CYBERWISER.eu	

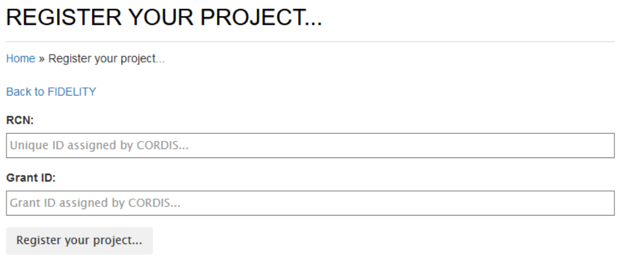
Step 3 - Access to you project mini page, find the Radar box at the bottom and add your request.



Your project in the Radar

- Add New Request

Click on “Add new request” and provide either the project’s RCN or Grant ID as provided by CORDIS. Click on “Register your project”.



REGISTER YOUR PROJECT...

Home » Register your project...

Back to FIDELITY

RCN:

Unique ID assigned by CORDIS...

Grant ID:

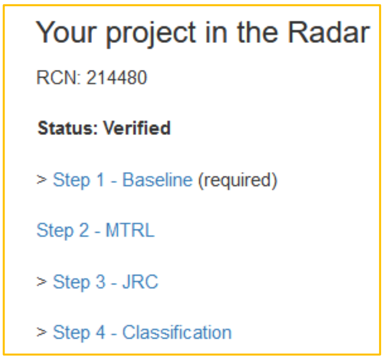
Grant ID assigned by CORDIS...

The system will redirect you to your Project page in the "Your Project in the Radar" box.

"Your Project in the Radar" box now presents a Status "Not Verified". For the activation of the Status, Cyberwatching.eu Team will manage it. You will receive an email notification once the Status is activated and you can proceed with the following steps.

Step 4 – Complete your project’s Baseline

Once the Status is activated you will be able to go to "Your Project in the Radar" box which now presents 4 links (Baseline MTRL, JRC, Classification).



Your project in the Radar

RCN: 214480

Status: Verified

> Step 1 - Baseline (required)

Step 2 - MTRL

> Step 3 - JRC

> Step 4 - Classification

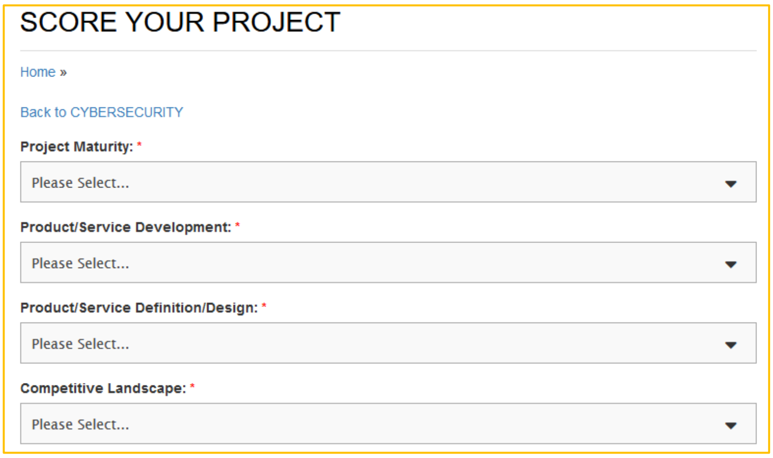
Click on "Baseline. Complete the required fields missing:

- Full Name – Your full name
- Email – Your email
- Project homepage -The project URL
- Funding body entry – The project CORDIS page URL
- CW ProjectHUB link – The Cyberwatching.eu project page URL

Click on “Edit your project” to finalise your project’s Baseline.

Step 5 - Self assess your project in terms of MTRL.

For each field just select the desired options from the drop-down menus. The Description field is not mandatory. Click on “Score it” to update the MTRL.



SCORE YOUR PROJECT

Home »

Back to CYBERSECURITY

Project Maturity: *
Please Select...

Product/Service Development: *
Please Select...

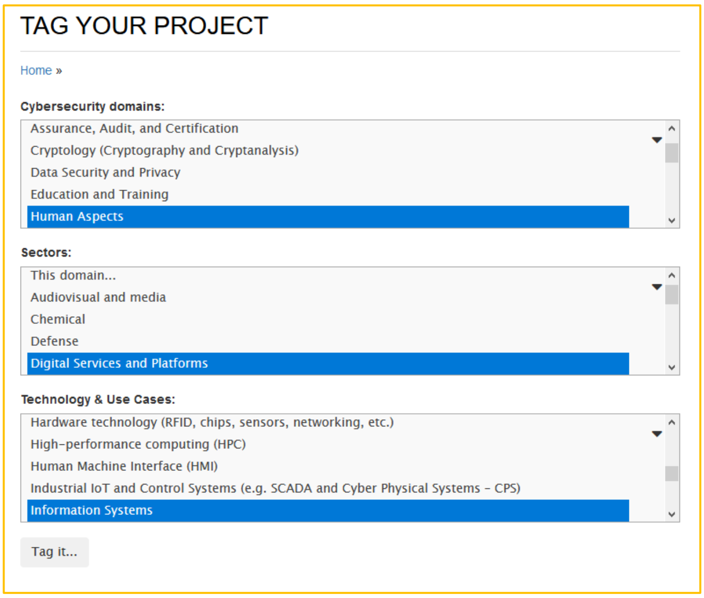
Product/Service Definition/Design: *
Please Select...

Competitive Landscape: *
Please Select...

Step 4 - Tag your project according to JRC

For each of the three main category (Cybersecurity domains, Sectors and Technology and Use Cases) you can choose one or multiple tags. To select and remove multiple tags, use the key combination CTRL+LeftClick or CMD+LeftClick.

Click on “Tag it” to apply the JRC tags.



TAG YOUR PROJECT

Home »

Cybersecurity domains:
Assurance, Audit, and Certification
Cryptology (Cryptography and Cryptanalysis)
Data Security and Privacy
Education and Training
Human Aspects

Sectors:
This domain...
Audiovisual and media
Chemical
Defense
Digital Services and Platforms

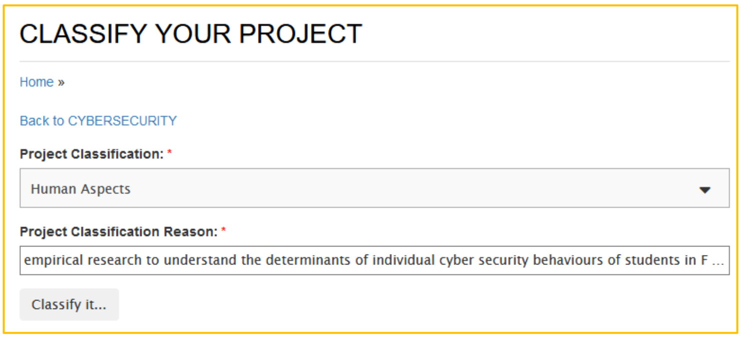
Technology & Use Cases:
Hardware technology (RFID, chips, sensors, networking, etc.)
High-performance computing (HPC)
Human Machine Interface (HMI)
Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS)
Information Systems

Tag it...

Step 5 - Classify your project based on Cyberwatching taxonomy

You can change the classification of your project by simply selecting the domain that best apply to it from the drop-down menu. It is mandatory to provide a Project Classification Reason to change the classification.

Click on “Classify it” to apply the new classification.



CLASSIFY YOUR PROJECT

Home »

Back to CYBERSECURITY

Project Classification: *

Human Aspects

Project Classification Reason: *

empirical research to understand the determinants of individual cyber security behaviours of students in F ...

Classify it...

Projects are positioned in sections according to the Cyberwatching.eu taxonomy describing specific cybersecurity research and innovation sub areas:

-Operational risk: Understanding the risk and harm resulting from cyberattacks, and how it propagates across and between organisations. Work focuses on creating situational awareness through aiming for a complete understanding of scenario and risk management; metrics and models for security postures; and analytics for predicting risk, prioritising responses and supporting security operations.

-Verification and assurance: Two disciplines that help establish how much confidence you can have in a system, both in terms of security and the privacy of all stakeholder groups who act with or in a system. Assurance focuses on managing risks related to the use, processing, storage, and transmission of information, whereas formal verification seeks to build a mathematical model of a digital system and then try to prove whether it is ‘correct’, often helping to find subtle flaws.

-Secure systems: How security can be built into technology from the design stage including cloud computing security, cryptography, trusted platforms, wireless security, mobile security and secure coding paradigms.

-Identity and Privacy: Bringing diverse perspectives and interpretations to questions such as: Who are you online, how do you communicate, and what can (or should) you do? This also connects to the ongoing activities on Privacy launched through directives and regulations over the past years.

- Cybersecurity governance: Looking at politics, international relations, defence, policy and governance issues: how do countries and communities interact with (and through) technology, and how might this change in different contexts?

-Human aspects: Understanding the ways humans interact with (and through) digital systems whether to understand and design for target users, or to understand how adversaries operate and can exploit the systems. This includes aspects like usability, trust, collaborative practices, social embeddedness, nationhood, cultural diversity, impact on economy, and the relationship between microsocial interactions and global structures.