



## How to prepare your SME against cybersecurity risks and threats

10 January 2024, 09:52

Tatiana Galibus

### Start activating your cybersecurity skills!

At Sirris, we often work with companies that are stepping into connectivity (Industry 4.0 transition) or starting to use or develop digital services (digital transition). The increased connectivity and data exchange at the heart of these transitions introduce new types of risks and threats, particularly for SMEs. Without a proper cybersecurity strategy the opportunities of these transitions cannot be exploited by Belgian companies.

**In September 2023 we launched a new cybersecurity project – [CyberActive](#) – with the ambition to improve the cybersecurity literacy in SMEs and related target groups (especially for the manufacturing and digital service sectors).**

The goal of this project is to develop and deliver material to increase the active CS skills of these target groups, so they can build and start to execute their cybersecurity (CS) strategy. The novelty of the Cyberactive trainings campaign is its granular case-specific orientation. Trainings materials are focused on the practical cybersecurity skills often lacking in the industry: specific modules for the ICT administrators, for the operators and maintenance technicians, for the certification bodies, for the developers, for the support team etc.

We will be giving regular cybersecurity sessions, starting from January 2024. The sessions will be conducted online and in physical locations, and will cover the following topics:

For manufacturing:

- IMPLEMENT cybersecurity on the connected shopfloor
- FORTIFY digital defences in manufacturing
- STRENGTHEN resilience against phishing and targeted threats

For digital services:

- STEP INTO NIS2 compliance and resilience against phishing
- LEARN TO BUILD trusted digital services by stepping into application security and DevSecOps

Each session will last 2 hours and cover two topics. We will dedicate the last 30 min to Q&A with the experts.



## Authors



Tatiana Galibus