PRESENTATION OF THE CYBER CAMPUS

WORKSHOP ON SHARING OF CYBER SECURITY SOLUTIONS FOR MSMEs

G20, FEBRUARY 13TH 2023

CYBERSECURITY CONTEXT

WHAT ANSSI HAS OBSERVED

1 THE NUMBER OF CYBER-ATTACKS IS INCREASING EVERY YEAR

2 IT AFFECTS BOTH CITIZENS AND BUSINESSES

3 THE OVERALL LEVEL OF ATTACKS REMAINS HIGH

THREATS ARE EVOLVING **4**

| They affect less and less regulated operators | They are redirected to less well protected entities | They seek to obtain discrete and permanent access to their victims' networks |

5

IN 2021 AND 2022, THE MAIN FRENCH VICTIMS OF RANSONWARE ATTACKS WERE MSMEs, LOCAL GOVERNMENTS AND PUBLIC HEALTH INSTITUTIONS

CREATION AND CONCEPT

A multistakeholder initiative launched at the beginning of 2022 with two main objectives :

1. To address the **specific needs of the cybersecurity ecosystem**

2. While **bringing together the stakeholders** of this ecosystem

Cyber Campus specificities :

- **Strong public-private collaboration** : the Cyber Campus is a private company owned at 44% by public institutions and 56% by private shareholders

- Opportunity for **different actors** (industries, schools, researchers...) to **work together**. 30% of the space is dedicated **to collaboration between stakeholders.**

- **Open governance** model where **every organization is represented**, whatever their size

THE CAMPUS GOALS

EDUCATION

In France, approximately **15,000 positions are unfilled** in the cybersecurity sector

Some training courses are not sufficiently filled and forced to close due to the lack of candidates
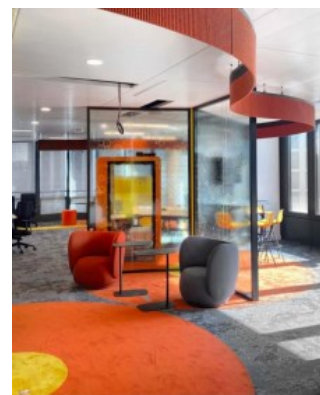
Cyber Campus hosts **EPITA**, one of France's major computer science engineering schools, as well as CFSSI – training center for information systems security. This way, Cyber Campus can **promote training courses relating to cybersecurity**

Goals :

Provide a place where **digital talents** and the skills of the future can **emerge** in order to **make up for the shortage of qualified human resources to fill digital jobs**

Supporting courses for a diverse public in order to **help the whole ecosystem to upskill**

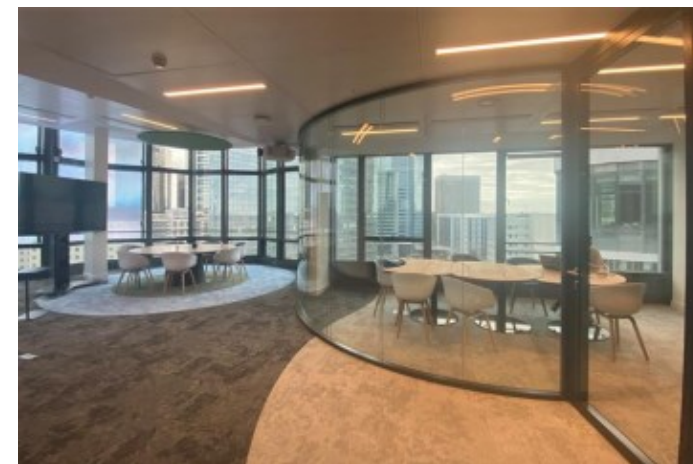Work is under way **to feminize cyber professions**

INNOVATION

| Foster more innovation | Help entrepreneurs to create new cybersecurity companies and accelerate their development | Ease exchange of information and expertise between startups, researchers, government, and large corporations | Facilitate collaboration between digital companies (private and public players) |

Examples of projects :

A **startup studio dedicated to cybersecurity** that will support more than **30 startups over the next 3 years**

Community work : Banks have decided to start joint work to strengthen their respective systems in order to better address the threat

Development of an Intelligence Base (CTI): Create a database sharing data to better anticipate the threat and strengthen our production systems

OPERATIONS

Promote **sharing of data and experiences**

In order to strengthen the ecosystem's capacity to handle cyber risks

NEXT STEPS

→ Recent legal developments (such as the new EU Directive on Network and Information System Security - NIS 2) will require a growing number of actors and in particular supply chain actors to strengthen their cybersecurity level

→ Cyber Campus is working on **labelling a network of regional cyber campuses** to **strengthen intra and inter territorial cooperation with the national level**