



*The Italian Avenue of Attack to
Cybersecurity skill shortage*

Paolo PRINETTO

CINI Cybersecurity National Lab

Paolo.Prinetto@cybersecnatlab.it

Mob. +39 335 227529



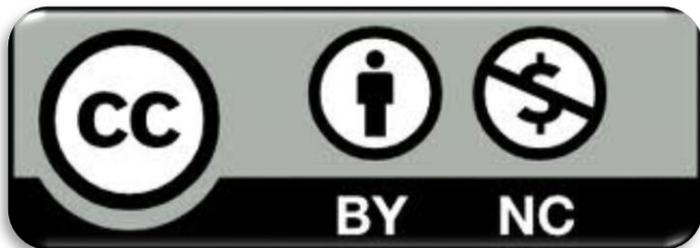
<https://cybersecnatlab.it>

License & Disclaimer

2

License Information

This presentation is licensed under the Creative Commons BY-NC License



To view a copy of the license, visit:

<http://creativecommons.org/licenses/by-nc/3.0/legalcode>

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.





A comprehensive and integrated set of *education* and *training* programs on various aspects of cybersecurity

THE BIG GAME

OF CYBERSECURITY

A comprehensive and integrated set of *education* and *training* programs on various aspects of cybersecurity
organized by



THE BIG GAME

OF CYBERSECURITY

A comprehensive and integrated set of *education* and *training* programs on various aspects of cybersecurity
organized by *under the patronage of*



&



GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

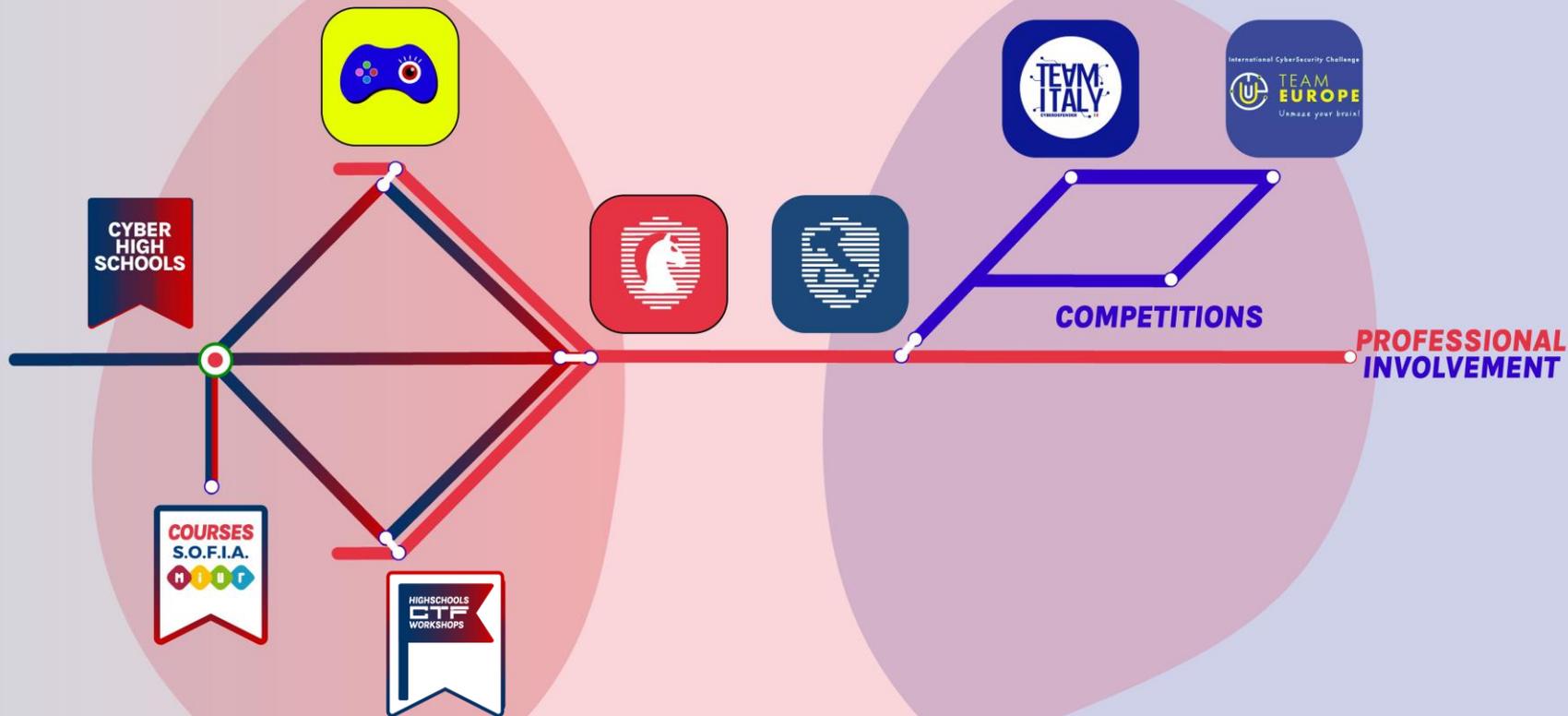


**CYBERSECURITY
NATIONAL LAB**

THE BIG GAME

OF CYBERSECURITY

-  Training
-  CTFs
-  CyberHighSchools





**CYBERSECURITY
NATIONAL LAB**

THE BIG

OF CYBERSECURITY

hools

*It fully implements
the Measure #65 of
the Italian National
Strategy on
Cybersecurity
2022-2026*



VAL
NT



**CYBERSECURITY
NATIONAL LAB**

THE BIG GAME

OF CYBERSECURITY

-  **Training**
-  **CTFs**
-  **CyberHighSchools**

All the programs
are always
completely free
for participants



COMPETITIONS

**PROFESSIONAL
INVOLVEMENT**



**CYBERSECURITY
NATIONAL LAB**

THE BIG GAME

OF CYBERSECURITY

-  Training
-  CTFs
-  CyberHighSchools

All the programs
are always
completely free
for participants

Thanks to all our
private and
public sponsors!

IAL
NT

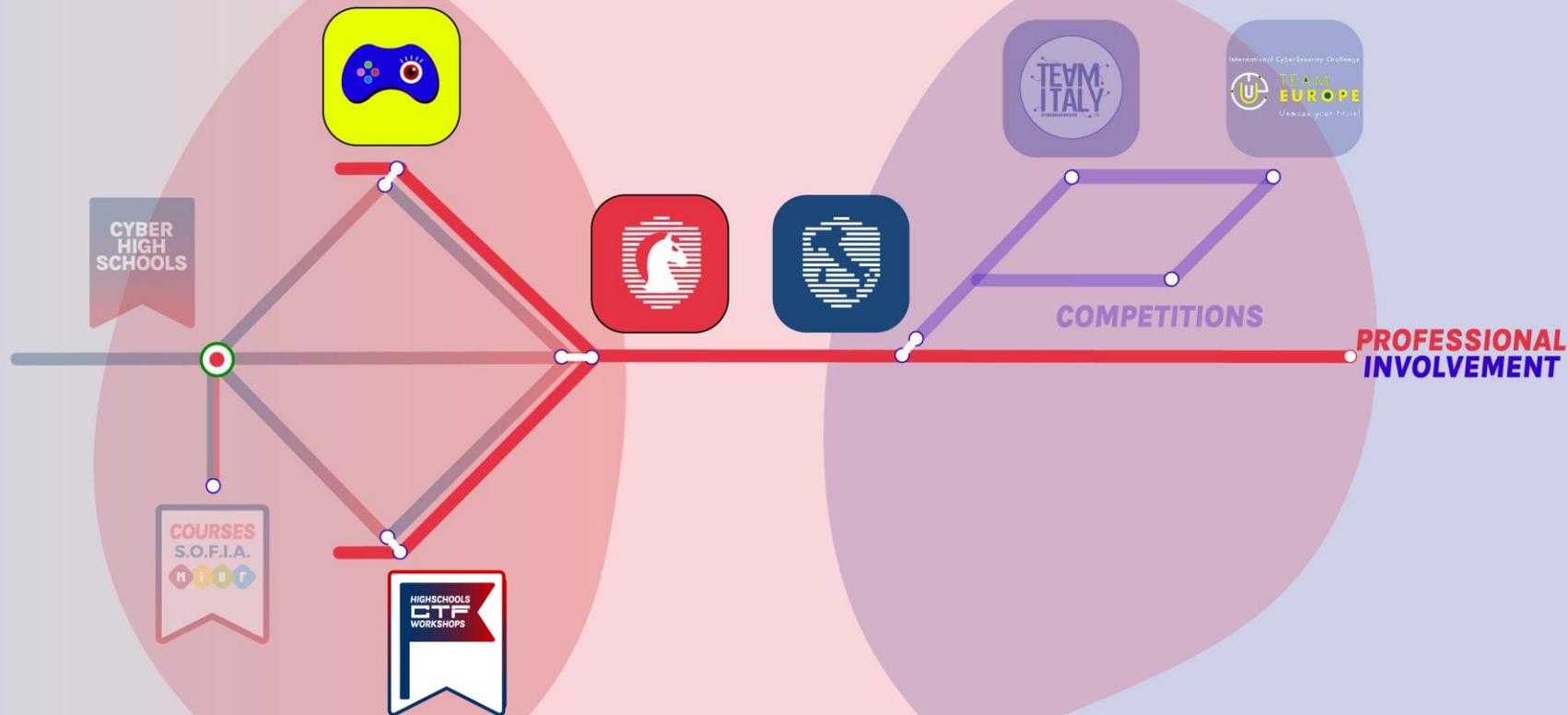


**CYBERSECURITY
NATIONAL LAB**

THE BIG GAME

OF CYBERSECURITY

-  Training
-  CTFs
-  CyberHighSchools



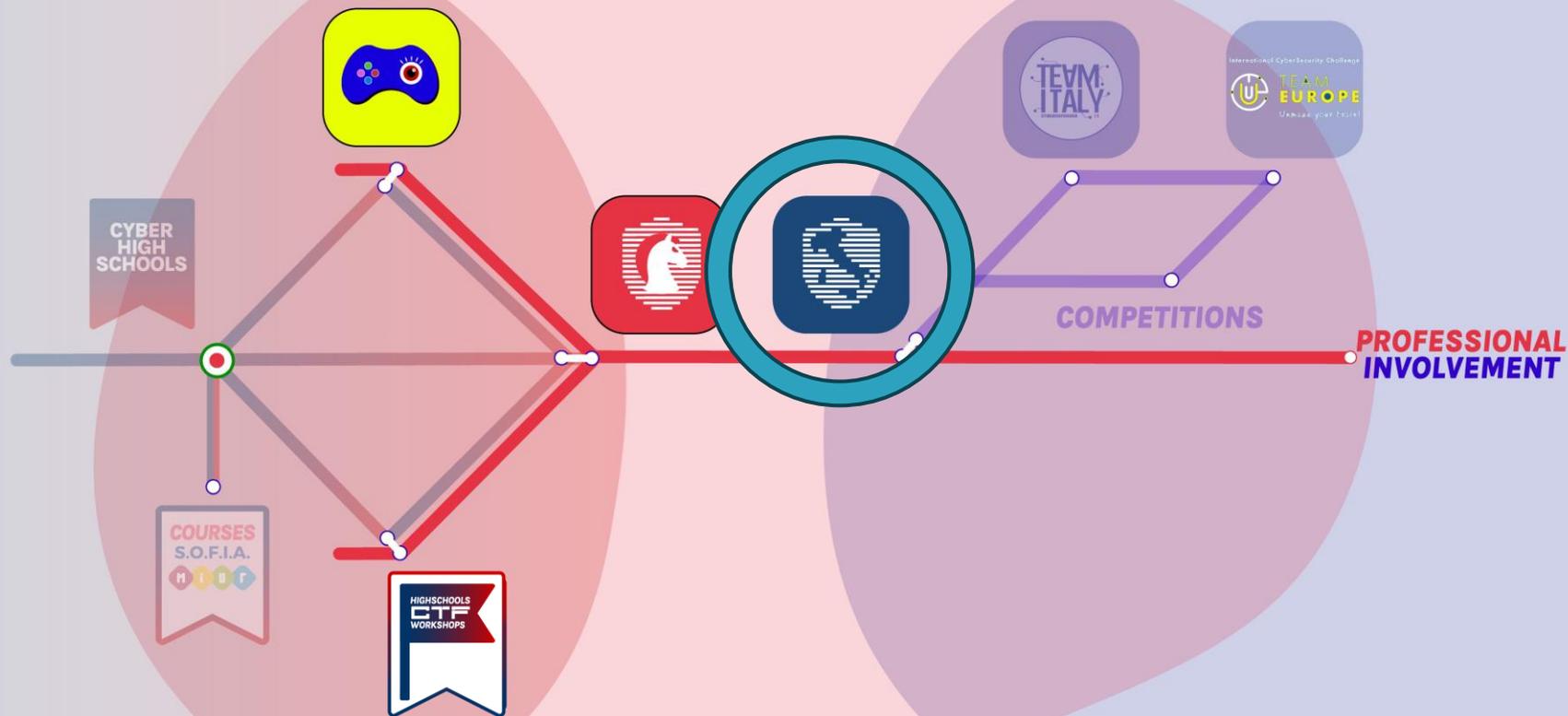


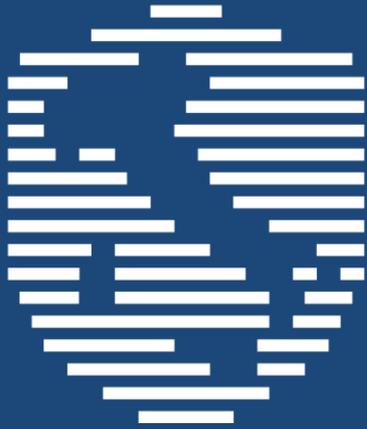
**CYBERSECURITY
NATIONAL LAB**

THE BIG GAME

OF CYBERSECURITY

- Training
- CTFs
- CyberHighSchools





CYBER
CHALLENGE.IT

cyberchallenge.it

- In 2017, prof. Roberto BALDONI launched the program with the goal of identifying and growing the best young talents (he was used to call them *the Formula 1 drivers*), to be exploited in critical situations and activities.



cyberchallenge.it

- In 8 year, *CyberChallenge.IT* has become the 1st Italian training program in cybersecurity for *high-school, undergraduate, and graduate students* (aged 16-24)



Up to now:

- **8** editions
- **29,270** enrolled
- **4,550** participants

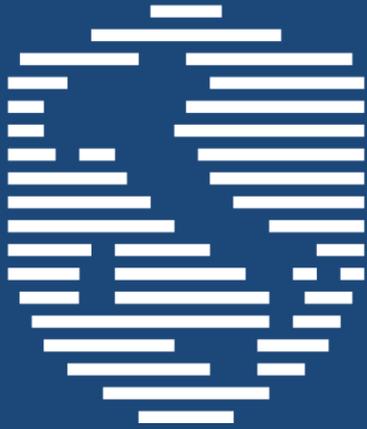
- In 8 year, *CyberChallenge.IT* has become the 1st Italian training program in cybersecurity for *high-school, undergraduate, and graduate students* (aged 16-24)

Up to now:

- **8** editions
- **29,270** enrolled
- **4,550** participants

The 2024 edition:

- **43** Locations/Teams
- **4,100+** enrolled
- **1,075** participants



CYBER
CHALLENGE.IT

cyberchallenge.it

Workflow

- *2 Admission Tests*
- *Team clustering* – 20 student/team
- *Training path* – 12 weeks, 6+ h/w
- *2 Final competitions* – CTF Jeopardy & Attack/Defense

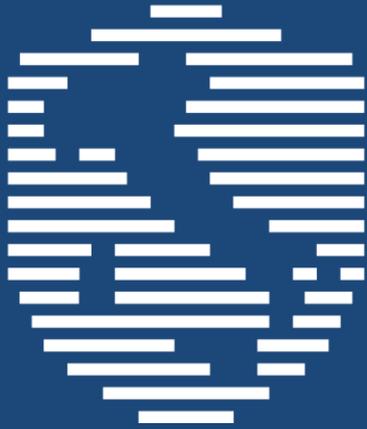


W

ts

V

ons —



CYBER
CHALLENGE.IT

cyberchallenge.it

- Issue:
 - The marginal involvement of *High Schools Students*

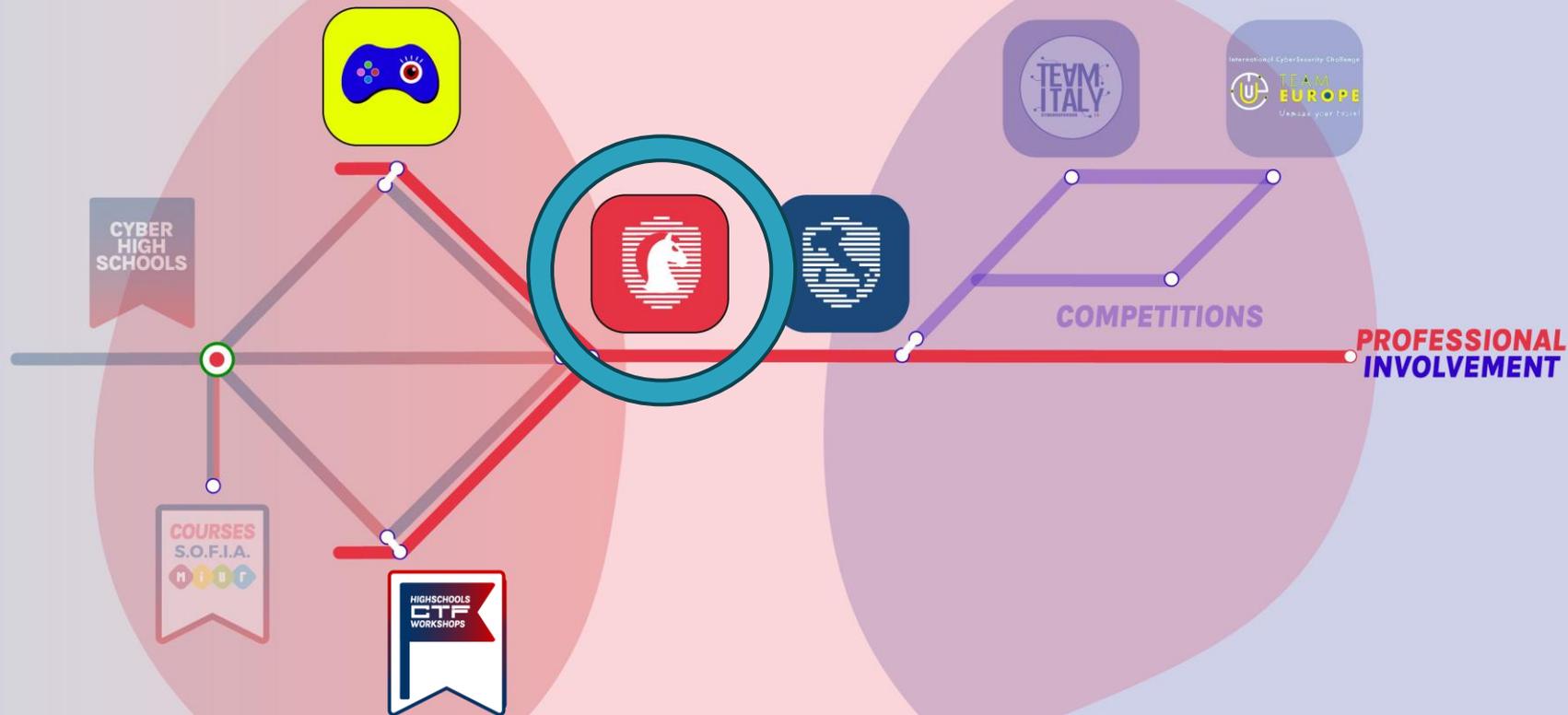


**CYBERSECURITY
NATIONAL LAB**

THE BIG GAME

OF CYBERSECURITY

- Training
- CTFs
- CyberHighSchools





OLIMPIADI
ITALIANE DI
CYBERSICUREZZA

olicyber.it

- Program aimed at fostering and encouraging the approach to cybersecurity of *students of any year of any Italian high school* (students in K-9 to K-13)



Up to now:

- *4 editions*
- ***11.430+** participants*

- Program aimed at fostering and encouraging the approach to cybersecurity of *students of any year of any Italian high school* (students in K-9 to K-13)



OLIMPIADI ITALIANE DI CYBERSICUREZZA

olicyber.it

- **Workflow:**
 - Admission test (~4.400 participants)
 - Regional CTF qualifier in an individual jeopardy format (~1.000 participants)
 - National CTF competition in a individual jeopardy format (100 participants)

CYB



400

er in
dy

ition
dy
(nts)





OLIMPIADI
ITALIANE DI
CYBERSICUREZZA

olicyber.it

- Issue:
 - The significant *Gender Gap*

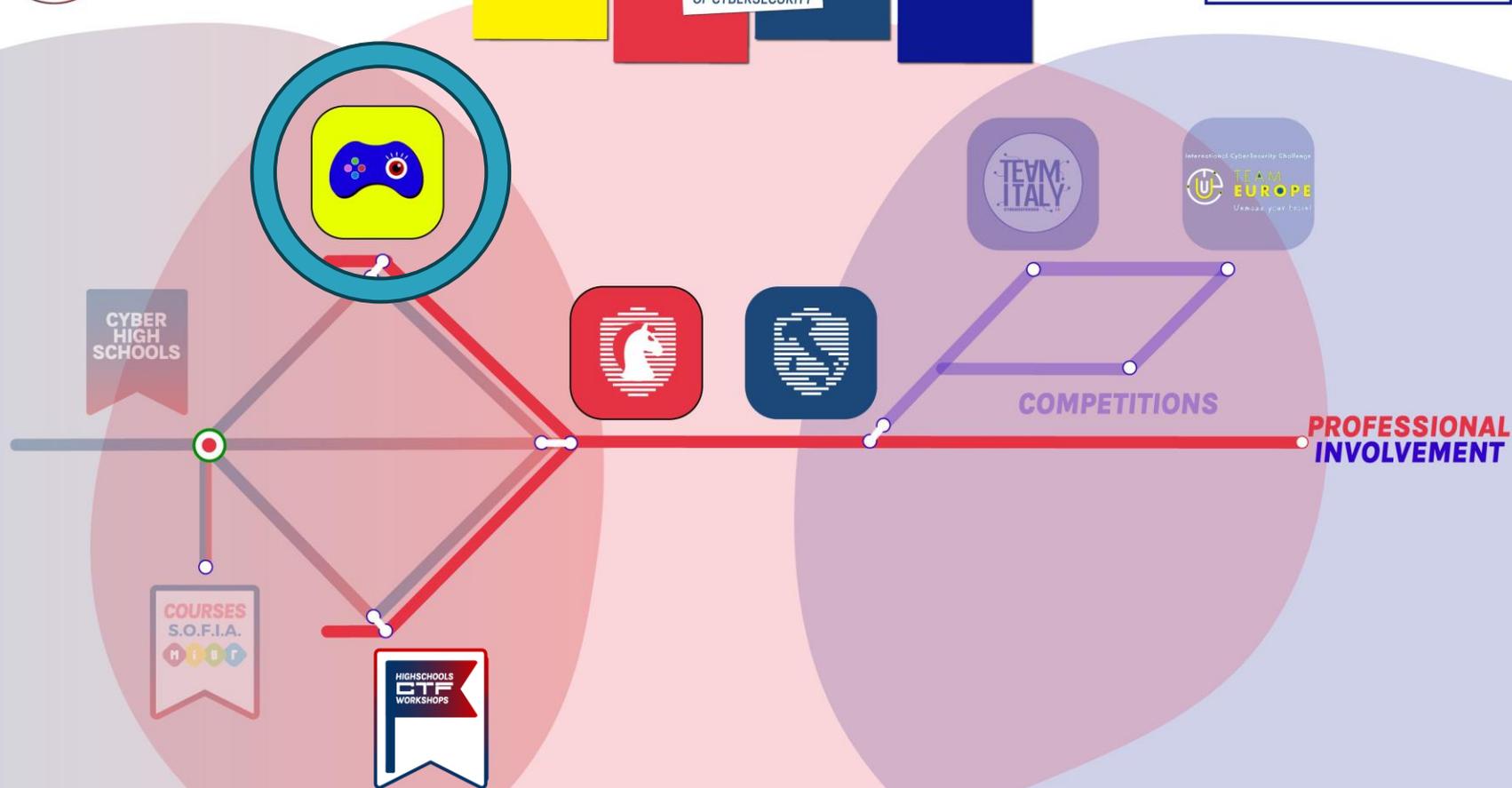


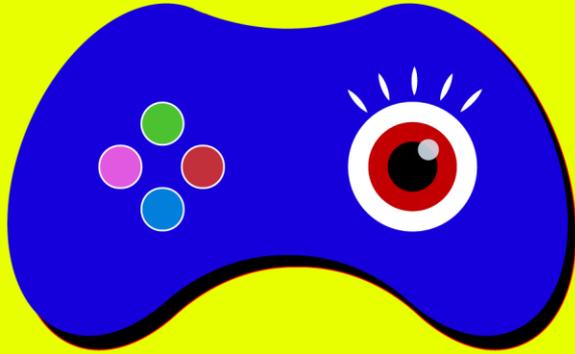
**CYBERSECURITY
NATIONAL LAB**

THE BIG GAME

OF CYBERSECURITY

- Training
- CTFs
- CyberHighSchools

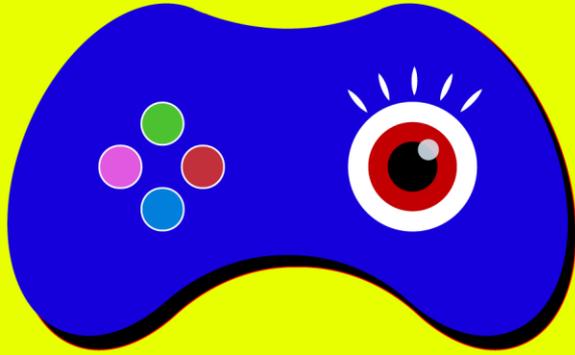




CYBERTRIALS

cybertrials.it

- Advanced training program for *female students at Italian high schools* (in K-9 to K-13)



CYBERTRIALS

cybertrials.it

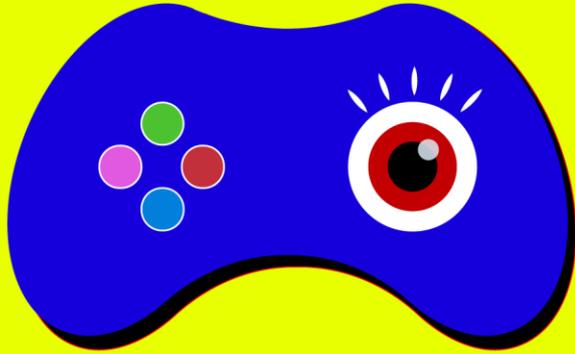
- Aimed at promoting online civic mindedness and at mastering several digital aspects, to *improve participants' online safety and security*



Up to now:

- **3** editions
- **2.050+** participants

- Aimed at promoting online civic mindedness and at mastering several digital aspects, to *improve participants' online safety and security*



CYBERTRIALS

cybertrials.it

- **2024 Edition:**
 - **800+ enrolled**
 - The top 16 teams (6 girls each) attended the *National Final Competition*, in Turin, June 3-5, 2024, at the ITC-ILO UN training Campus
 - Open to international participation



rls

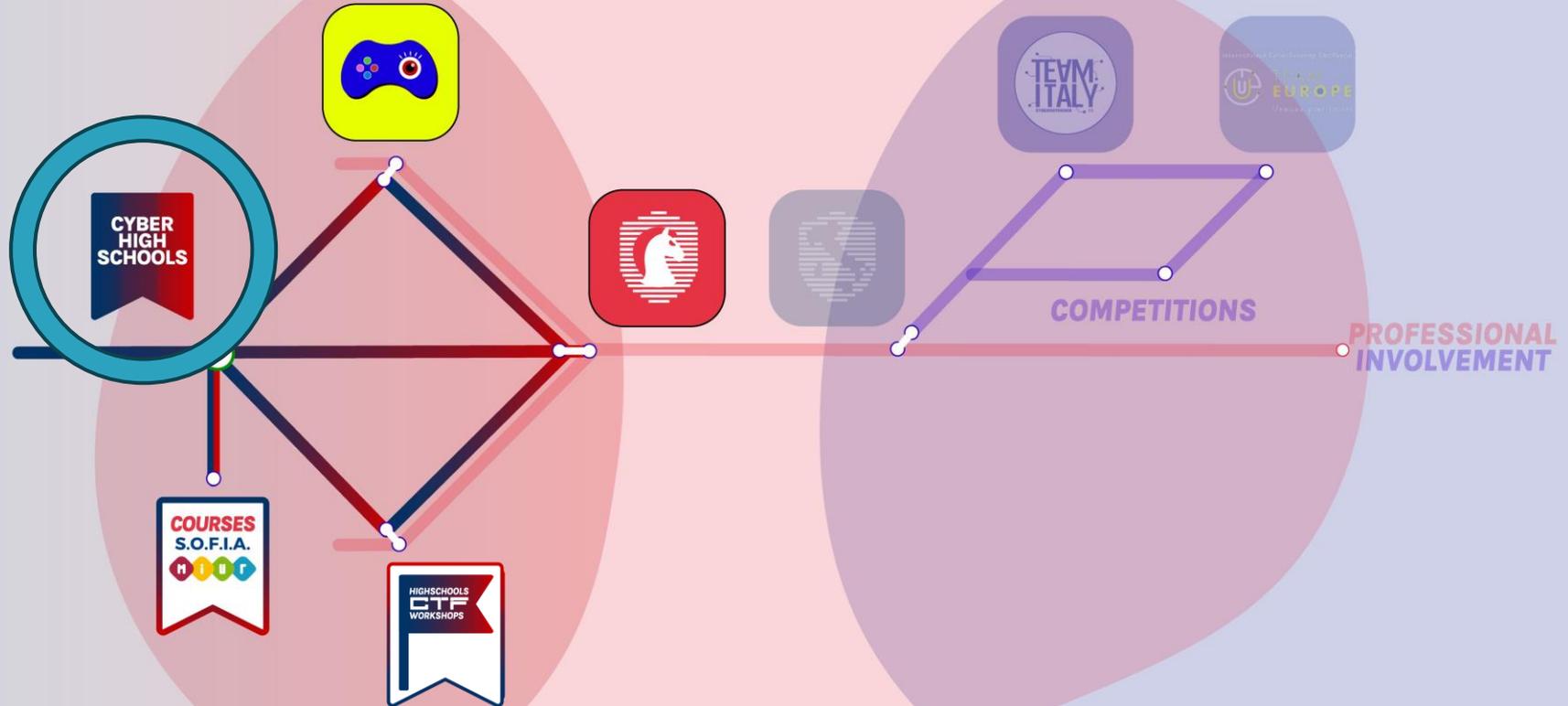


**CYBERSECURITY
NATIONAL LAB**

THE BIG GAME

OF CYBERSECURITY

- Training
- CTFs
- CyberHighSchools



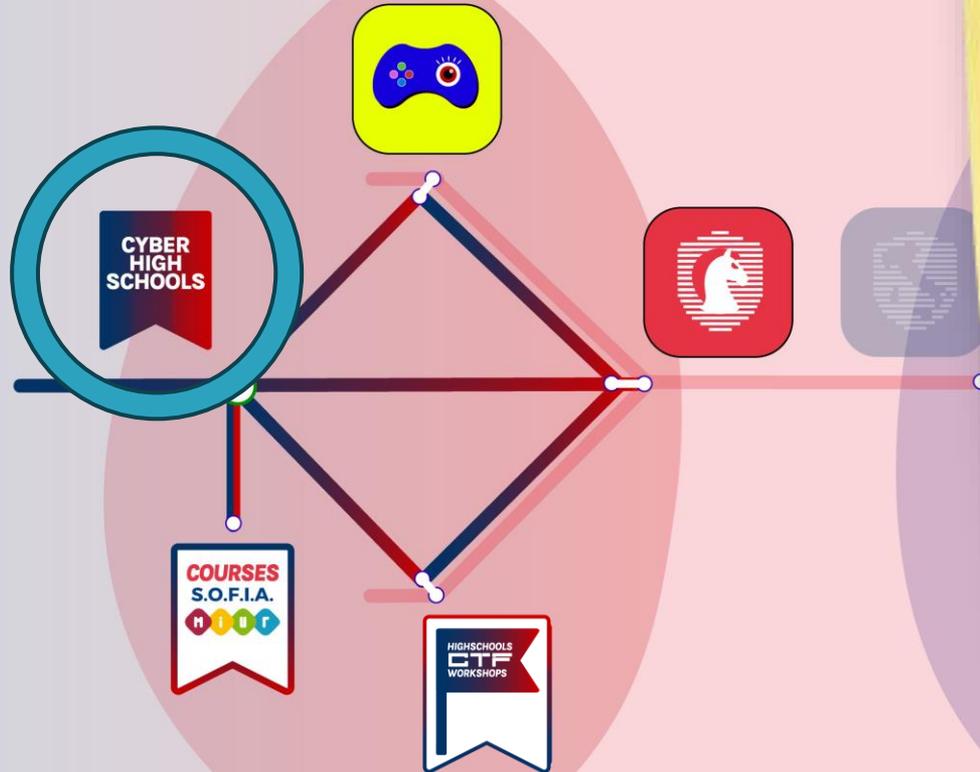


**CYBERSECURITY
NATIONAL LAB**

THE BIG GAME

OF CYBERSECURITY

- Training
- CTFs
- CyberHighSchools



The importance of
*Training the
Trainers*

NAL
ENT

The logo for Cyber High Schools is a white ribbon-like shape with a blue border and a red bottom edge. Inside the ribbon, the text "CYBER HIGH SCHOOLS" is written in a bold, sans-serif font. "CYBER" and "SCHOOLS" are in blue, while "HIGH" is in red.

**CYBER
HIGH
SCHOOLS**

cyberhighschools.it

- Program aimed at:
 - Delivering training courses for the professors

CYBER

*Up to now,
1,550+ professors
attended our
courses*

Completed:

- 9 editions of the
introductory
course*
- 11 editions of the
advanced course*

ECSC 2024



36

- From October 8 to 11, 2024, jointly with ACN, we shall organize the *ECSC 2024* competition in Turin, at the OGR location



ECSC 2024

37



ECSC 2024

HOME

EVENT ▾

OPENECSC ▾

PARTNERS

DOCS

NEWS

EUROPEAN CYBERSECURITY CHALLENGE 2024

The **European Cybersecurity Challenge** is the annual cybersecurity championship during which teams of 10 members aged 14 to 24, representing European and some invited non-European countries, participate on-site in cybersecurity competitions (CTF - Capture The Flag) over 2 days, to determine the European champion. The event, supervised by **ENISA**, the European Cybersecurity Agency, takes place annually in a different European country, which takes care of its organization. In 2024 it will take place in **Turin, Italy** from **October 7th to 11th**, and will be jointly organized by the Italian **National Cybersecurity Agency** and the **Cybersecurity National Lab**.



CYBER
NATIONAL



CYBERSECURITY
NATIONAL LAB



Road to...

ECSC 2024

Torino, 8-11/10/2024

openECSC

39

- 🔗 A worldwide cybersecurity competition open to everyone
- 🔗 Aimed to broaden participation beyond traditional age and nationality restrictions and to expands the ECSC community
- 🔗 Managed by the same organizers of ECSC 2024

openECSC

40

A worldwide competition

# Round	Starting time	Ending time
Round 1	18 Mar. 2024, 10:00 UTC	24 Mar. 2024, 22:00 UTC
Round 2	22 Apr. 2024, 10:00 UTC	28 Apr. 2024, 22:00 UTC
Round 3	13 May 2024, 10:00 UTC	19 May 2024, 22:00 UTC
Final Round	21 Sep. 2024, 10:00 UTC	22 Sep. 2024, 10:00 UTC

the organizers of ECSC 2024



openECSC

41

A worldwide

# Round	
Round 1	
Round 2	
Round 3	
Final Round	

- 3rd round:*
- **3.272 Participants**
 - **from 143 Nations**

Ending time
24, 22:00 UTC
24, 22:00 UTC
24, 22:00 UTC
24, 10:00 UTC

2024



Road to ECSC 24

42

- All the CTFs organized in 2024 by our Lab has been freely accessible and playable by every countries involved in ECSC
 - *CyberChallenge.IT:*
 - Local final: 300+ participants from 40+ nations
 - National final A/D: 30 national teams participant, including TeamItaly
 - *OliCyber:*
 - 250+ participants
 - *CyberTrials:*
 - 6 team
 - *TeamItaly*



Concluding remark

43

- *Gaming* is never an end in itself, but a very valuable path for involving young people and creating VERY significant skills, experiences, and expertise that can then be made available to the whole Country and to the entire community.





Paolo PRINETTO

CINI Cybersecurity National Lab

Paolo.Prinetto@cybersecnatlab.it

Mob. +39 335 227529



**CYBERSECURITY
NATIONAL LAB**

<https://cybersecnatlab.it>



Bridging the Cybersecurity Gap with Challenges and CTF

Part II: the context

Paolo Atzeni, ACN
p.atzeni@acn.gov.it

ECSF Budapest, 27/09/2024

Cybersecurity skill shortage and gap

- *The lack of qualified cybersecurity professionals in the labour market, represents an issue for both economic development and national security, especially in the rapid digitisation of the global economy (ENISA 2019)*

One goal, two (or three) faces

- Cybersecurity concerns everyone as information technologies are pervasive.
 - We need a significant number of cyber specialists
 - Those with responsibilities (at various levels) must know how to use and manage technologies, giving them the right value:
 - 'Right' means acceptance, awareness, a mature approach, not blind faith, and collaboration among individuals with diverse skills.
 - At the operational level, people need to know how to use technologies.
 - At progressively higher levels, knowing how to govern technologies is necessary, overseeing those who use them and engaging with those who promote and develop them.

Cyber skills, three perspectives

1. Basic level, risk awareness (cybersecurity awareness culture)
2. Specialized cybersecurity skills (from a technological or legal/administrative/management perspective)
3. "Complementary skills" for
 - officials and executives at various levels, who have responsibilities regarding the security of activities within their own structures
 - specialists in application domains (healthcare, research, finance, law, infrastructure)

2. Educating specialists

- Systematic approach, with a mid term goal
 - Increase the number of cyber (or at least ICT, with cyber specialization) graduates
 - Requires time and effort (strong promotion of programs)
- More pragmatic approach (followed in ICT in the 1980s and 1990s)
 - Re-train or train on the job people with diverse background
 - Non-cyber ICT graduates
 - Non-ICT graduates

3. "Complementary skills" - A crucial issue

- A major misunderstanding
 - Often computer or cyber specialists think that studying methodologies and technologies is enough to apply them to any domain
 - Many of other stakeholders think that technologies are "commodities," such as water, electricity and gas, they can be used without any prior knowledge
- Unfortunately (or fortunately!) things are different
 - Computer specialists must understand application domains and policy
 - Stakeholders require knowledge of technology principles to use it effectively

Cybersecurity is not an island

- We need dialogue between specialists and domain experts
 - Cyber specialists should study and experiment with application domains
 - Education should consider topics that allow lawyers, managers, humanists to communicate with technology specialists

Competitions have a major role

1. More people hear about cybersecurity:
 - contribution to cybersecurity awareness
2. Some (hopefully many) people could be attracted to a cybersecurity career
 - contribution to the reduction of the skills shortage, search for technical talents
3. More people understand that cybersecurity is important, even if in the end they do not pursue a cybersecurity career
 - promotion of crossfertilization and of crossdisciplinary dialogue



Thanks

p.atzeni@acn.gov.it

www.acn.gov.it