Programma CyberChallenge.IT 2022 – *Presentazione generale*

Indice

CINI Cybersecurity National Lab
c/o DIAG - Sapienza Università di Roma
Via Ariosto, 25 – 00185 Roma RM
https://cybersecnatlab.it

Contatti:
segreteria.cybersecurity@consorzio-cini.it
https://cyberchallenge.it

1 Introduzione

Questo documento ha l'obiettivo di presentare l'edizione 2022 del programma di formazione CyberChallenge.IT[1], organizzato e gestito dal Laboratorio Nazionale Cybersecurity[2] del CINI.

2 Il programma

2.1 Presentazione

2.1.1 Missione

CyberChallenge.IT è un programma di formazione per i giovani talenti che punta a ridurre significativamente l'odierna carenza della forza lavoro in ambito informatico, ponendosi come la principale iniziativa italiana per identificare, attrarre, reclutare e collocare la prossima generazione di professionisti della sicurezza informatica, incoraggiandoli a riempire i ranghi dei futuri professionisti della cybersecurity, mettendo così le loro capacità a disposizione del sistema Paese.

2.1.2 Riconoscimenti istituzionali

Il programma si inserisce all'interno dell'Indirizzo Operativo n. 3 del "*Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*", guidato dal Sistema di Informazione per la Sicurezza della Repubblica - Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei Ministri.

Il programma è supportato dall'ACN - Agenzia per la Cybersicurezza Nazionale e ha il patrocinio del Ministero della Difesa.

A partire dal 2018, il Nucleo di Sicurezza Cibernetica (NSC) ha affidato al Laboratorio Nazionale di Cybersecurity del CINI il compito di organizzare e gestire le attività di TeamItaly, la Nazionale Italiana di Cyberdefender e di curarne, tra l'altro, la partecipazione alle competizioni internazionali del settore (vedi Sez. 4).

Dal 2020 Cyberchallenge.IT è stato riconosciuto dal Ministero dell'Istruzione come "*Progetto per la valorizzazione delle eccellenze*". Gli studenti delle scuole secondarie di secondo grado che otterranno risultati elevati nel programma possono accedere ai riconoscimenti e ai premi previsti dall'articolo 4 del d. lgs. 29 dicembre 2007, n. 262.

Per la realizzazione di alcune delle esercitazioni previste dal programma è previsto l'uso di Cyber Range ibridi, identificati come strumenti necessari "per la formazione e l'addestramento sul campo" dal PNR 2021-2027[3].

2.1.3 A chi è rivolto

I candidati sono giovani fra 16 e 24 anni che studiano nelle scuole secondarie di secondo grado e nelle Università italiane.

Per l'edizione 2022, le iscrizioni sono aperte ai giovani nella fascia di età compresa tra i 16 e i 24 anni compiuti nel 2021, vale a dire per i nati negli anni 1997-2005; l'iscrizione è gratuita.

---

[1] https://cyberchallenge.it

[2] https://cybersecnatlab.it

[3] Articolazione 6 del Grande Ambito Sicurezza, Ambito tematico Cybersecurity

2.1.4 Obiettivi

Il programma mira a creare e far crescere la comunità dei cyberdefender investendo sui giovani. In particolare, punta a:

- stimolare l'interesse verso le materie tecnico scientifiche e, in particolare, verso l'informatica;
- far conoscere le opportunità professionali offerte dai percorsi formativi sulla sicurezza informatica;
- mettere i giovani in contatto diretto con realtà aziendali, anche grazie alle sfide che saranno chiamati ad affrontare;
- identificare i giovani talenti cyber e contribuire al loro orientamento e alla loro formazione professionale.

2.1.5 Metodologia e contenuti formativi

Gli studenti vengono selezionati, a seguito di informazione capillare nelle scuole secondarie di secondo grado e nelle università, tramite due test, svolti entrambi on-line da remoto e finalizzati, rispettivamente a una prima selezione e alla composizione delle squadre.

Il programma di formazione affianca un'attività formativa tradizionale a un approccio orientato alla *gamification*, che si traduce nella partecipazione a competizioni in arene virtuali che simulano scenari di reti e ambienti operativi reali. Il modello proposto è unico nel suo genere nel panorama internazionale; esso, infatti, prevede non solo il ricorso al *gaming* come strumento di attrazione per i giovani, ma anche un significativo percorso formativo multidisciplinare. Tale percorso è incentrato sull'introduzione tecnica, scientifica ed etica alle tematiche connesse alla sicurezza informatica.

L'edizione 2022 offrirà agli studenti selezionati e suddivisi per sedi partecipanti, corsi di addestramento, che, a seconda delle sedi e nel rispetto delle restrizioni locali vigenti a causa del Covid, potranno essere in presenza o on-line da remoto.

L'edizione 2022 culminerà nel *quinto campionato italiano Capture-The-Flag (CTF) in cybersecurity,* che si svolgerà a Torino, presso *l'International Training Centre of the ILO*[4] il 7 e 8 luglio 2022 e permetterà sia di determinare la squadra vincitrice, sia di identificare la *Squadra Nazionale di Cyberdefender* che parteciperà alla European Cyber Security Challenge (ECSC)[5].

Per gli studenti delle scuole secondarie di secondo grado partecipanti al programma è possibile l'attivazione di *Percorsi per le competenze trasversali e per l'orientamento* e numerosi Atenei riconoscono Crediti Formativi Universitari (CFU) ai partecipanti al programma.

2.2 Ruolo dei principali stakeholder

Per quanto detto sopra, il progetto CyberChallenge.IT vede coinvolti molteplici attori che, sinergicamente, contribuiscono all'organizzazione, al finanziamento, alla visibilità e al successo dell'iniziativa, tra i quali vanno evidenziati:

- *Laboratorio Nazionale Cybersecurity del CINI*
- *ACN - Agenzia per la Cybersicurezza Nazionale*
- *Ministero della Difesa*
- *Ministero dell'Istruzione*

[4] https://www.itcilo.org/it

[5] https://www.europeancybersecuritychallenge.eu

- *Ministero dell'Università e della Ricerca*
- *Sistema Universitario Italiano*
- *Aziende private.*

In particolare, il *Laboratorio Nazionale Cybersecurity* opera da coordinatore dell'intero progetto, ne gestisce le diverse fasi, che vanno dalla promozione alla gestione quotidiana, e garantisce la qualità dei percorsi formativi. Il Laboratorio, inoltre, mantiene i contatti con le sedi universitarie e con i diversi stakeholder che aderiscono al progetto. Il Laboratorio contribuisce anche al finanziamento, mettendo a disposizione proprio personale e proprie attrezzature.

Siccome sta emergendo sempre più che la cybersecurity e quindi la disponibilità di figure professionali in grado di garantirla sono essenziali per la Sicurezza del nostro Paese, il progetto beneficia della collaborazione con l'ACN - Agenzia per la Cybersicurezza Nazionale, che considera il progetto in linea con quanto previsto dal *Piano Nazionale per la protezione cibernetica e la sicurezza*.

Dal 2020 il *Ministero dell'Istruzione* ha riconosciuto Cyberchallenge.IT come "*Progetto per la valorizzazione delle eccellenze*". Gli studenti delle scuole secondarie di secondo grado che otterranno risultati elevati nel programma possono accedere ai riconoscimenti e ai premi previsti dall'articolo 4 del d. lgs. 29 dicembre 2007, n. 262. Promuove inoltre il progetto, anche attraverso avvisi mirati, e contribuisce al supporto delle attività nell'ambito di *Percorsi per le competenze trasversali e per l'orientamento*.

Ovviamente il progetto si avvale della collaborazione dei diversi attori del *Sistema Universitario Italiano*: nell'edizione 2021 sono state ben 31 le sedi universitarie che hanno aderito al progetto. Le singole università utilizzano il progetto anche come un'occasione per pubblicizzare le proprie lauree in discipline informatiche e, soprattutto, forniscono supporto allo svolgimento del percorso formativo, in termini di spazi e di personale docente coinvolto. Significativo, al riguardo, anche il ruolo dei *Centri di Competenza Regionali in Cybersecurity* che stanno ora nascendo in diverse regioni italiane come forma di collaborazione tra università e centri di ricerca per attività di ricerca e supporto alle imprese e alla pubblica amministrazione locale.

Come è noto, la carenza di esperti in sicurezza informatica sta mettendo in difficoltà tante aziende a livello internazionale e l'Italia non è un'eccezione. Per questo assistiamo con piacere alla disponibilità di varie *Aziende Private* a supportare economicamente, attraverso sponsorizzazioni e in alcuni casi anche attraverso la messa a disposizione di competenze specifiche e di rilevanti casi di studio industriali, per l'attività formativa. In cambio, le aziende possono accedere ai curriculum dei giovani selezionati per la formazione e hanno l'opportunità di incontrarli in occasione di eventi mirati, organizzati on-line in occasione delle gare locali e di quella nazionale.

2.3 Benefici per i partecipanti

2.3.1 Benefici per gli studenti

Tra gli aspetti più rilevanti come ritorno per gli studenti partecipanti al programma vanno certamente evidenziati:

- Dal 2020 Cyberchallenge.IT è stato riconosciuto dal Ministero dell'Istruzione come "*Progetto per la valorizzazione delle eccellenze*". Gli studenti delle scuole secondarie di secondo grado che otterranno risultati elevati nel programma possono accedere ai riconoscimenti e ai premi previsti dall'articolo 4 del d. lgs. 29 dicembre 2007, n. 262;
- Approfondimento di argomenti di cybersicurezza;
- Percorso di formazione, riconosciuto, in termini di crediti formativi, da molte Università e Istituti Superiori di II grado del Paese;

- Accesso a un ampio materiale didattico, predisposto e rivisto da esperti, tutto in lingua inglese;
- Incontro con attori pubblici e privati del panorama della cybersicurezza nazionale;
- Incremento di visibilità verso aziende e istituzioni, condividendo il CV attraverso una piattaforma dedicata;
- Opportunità di effettuare *Stage* e *Internship* presso aziende del settore, significative istituzioni nazionali, e sedi del Laboratorio Nazionale di Cybersecurity dislocate sul territorio nazionale;
- Possibilità di ricevere, al termine del percorso di formazione, sia *attestati di partecipazione* rilasciati dal Laboratorio Nazionale, sia degli *Open Badge*[6], fruibili tramite la piattaforma Bestr[7] del CINECA.

2.3.2 Benefici per le sedi universitarie

Tra gli aspetti più rilevanti come ritorno per le sedi universitarie partecipanti al programma vanno evidenziati:

- Entrare a far parte del network CyberChallenge.IT, come sede presso la quale gli studenti possono partecipare al programma;
- Incrementare la propria capacità attrattiva verso gli studenti delle Scuole Superiori del territorio;
- Accedere a un ampio e approfondito materiale didattico, predisposto e rivisto da esperti, con la possibilità di utilizzo del medesimo per fini didattici istituzionali, a seguito della stipula di appositi accordi;
- Accedere, in modalità remota, al CyberRange *Paideusis* (παίδευσις) attivato grazie a un progetto congiunto Lab. Naz. Cybersecurity del CINI e Fondazione Links, presso il quale sarà possibile svolgere le esercitazioni relative ad alcuni dei moduli del programma (e.g., Network Security e Hardware Security);
- Offrire agli studenti coinvolti:
    - opportunità di incontro con significativi attori pubblici e privati del panorama della cybersecurity nazionale;
    - la possibilità di incrementare la propria visibilità verso aziende e istituzioni, tramite la condivisione del proprio CV attraverso una piattaforma dedicata;
    - opportunità di effettuare *Stage* e *Internship* presso aziende del settore, significative istituzioni nazionali, e sedi del Laboratorio Nazionale di Cybersecurity dislocate sul territorio nazionale;
    - opportunità di essere convocati a far parte di TeamItaly, la Nazionale Italiana di Cyberdefender, e di partecipare anche a competizioni internazionali del settore;
- Opportunità di poter utilizzare, per l'eventuale erogazione del percorso formativo in modalità remota, di piattaforme messe a disposizione dal Lab. Naz. Cybersecurity.

[6] https://openbadges.org

[7] https://bestr.it

2.3.3 Benefici per gli Sponsor

Tra gli aspetti più rilevanti come ritorno per le aziende e gli enti che intendono sponsorizzare il programma vanno certamente evidenziati:

- Incremento della propria visibilità in operazioni socialmente rilevanti e di impatto per il grande pubblico, con una spiccata evidenza nel panorama istituzionale italiano ed europeo, come dimostrato dalla eco mediatica delle edizioni precedenti. In particolare, la visibilità è garantita attraverso:
  - i media, il sito web e i profili social del programma;
  - la piattaforma di formazione;
  - il materiale divulgativo ufficiale del programma;
  - gli eventi ufficiali; in particolare sono organizzati, a livello sia locale sia nazionale, degli incontri con le aziende, per consentire ai partecipanti al progetto di conoscere le aziende che lo hanno sponsorizzato, dando l'opportunità alle aziende stesse di illustrare iniziative per giovani di talento e stabilire contatti diretti con loro, in occasione delle cerimonie di premiazione. È prevista inoltre la partecipazione all'evento di premiazione finale nazionale con la possibilità di intervenire con un Plenary Talk di fronte a VIP e autorità istituzionali.
- Ampliamento della propria rete di contatti con l'accademia e gli enti governativi, in maniera integrata e sinergica;
- Accesso a un bacino di oltre 600 profili di giovani talenti, selezionati a partire da una base di alcune migliaia e formati grazie a un impegnativo percorso presso oltre 30 sedi universitarie, distribuite su tutto il territorio nazionale;
- Possibilità di pubblicizzare offerte di lavoro e/o opportunità di internship/stage all'interno dell'azienda tramite il portale del programma, in una sezione dedicata, accessibile a tutti;
- Possibilità, per un certo numero di propri dipendenti, di poter partecipare a una competizione di tipo Capture-the-Flag in stile Jeopardy riservata ai soli dipendenti delle ditte sponsor. I primi 3 classificati della competizione verranno premiati durante la Cerimonia di Premiazione nazionale.

2.4 Fasi di svolgimento

Ciascuna edizione del programma CyberChallenge.IT prevede:

1. L'adesione al programma da parte delle Università, delle Scuole Superiori e degli sponsor, tramite il portale www.cyberchallenge.it.
2. L'*iscrizione* (gratuita) al programma da parte degli studenti interessati, tramite il portale www.cyberchallenge.it.
3. La possibilità di *training al test di ammissione* tramite la piattaforma che sarà utilizzata per il test; questa permette agli studenti iscritti di accedere sia agli esercizi delle edizioni precedenti sia a una simulazione dei test.
4. Un *test di ammissione* volto a selezionare studenti con eccellenti capacità logiche, di problem-solving e informatiche.
   Il test di ammissione si svolge in due fasi:
   a. Primo test on-line che, se superato, consente l'accesso al successivo;
   b. Secondo test on-line, svolto contemporaneamente in tutta Italia, che porta a selezionare un gruppo di 20 partecipanti per ciascuna sede.
5. Un *percorso formativo* mirato a fornire le basi metodologiche e pratiche richieste per analizzare vulnerabilità e possibili attacchi, identificando le soluzioni più idonee a

prevenirli, in ambiti diversi della cybersecurity. Il percorso ha una durata complessiva di circa 72 ore distribuite su quattro mesi e viene svolto on-line, gestito da ciascuna sede in orari compatibili con le attività didattiche degli studenti. Ogni sede erogherà la formazione in linea con le normative e le possibilità locali.

6. Una *gara CTF locale individuale,* mirata a selezionare i migliori studenti di ciascuna sede. Gestita dalle singole sedi in contemporanea con le altre, alla gara segue una premiazione locale e una recruitment fair on-line o in presenza in cui gli studenti hanno l'opportunità di incontrare gli sponsor locali.
7. *Una gara CTF nazionale a squadre* (una squadra per ciascuna sede locale). A valle della gara sono previsti:
    a. una *cerimonia di premiazione nazionale* presieduta da rappresentanti delle istituzioni italiane;
    b. un *incontro con le aziende*, in cui i giovani incontrano le aziende sponsor a livello nazionale.
8. *La selezione di 20 partecipanti chiamati a far parte di TeamItaly,* la Squadra Nazionale Italiana di Cyberdefender che rappresenta l'Italia nelle competizioni internazionali.

2.5 Percorso formativo

Il *percorso formativo* mira a fornire le basi metodologiche e pratiche richieste per analizzare vulnerabilità e possibili attacchi, identificando le soluzioni più idonee a prevenirli, in ambiti diversi della cybersecurity. In particolare, è organizzato in *Aree Tematiche*, a loro volta organizzate in *Moduli*, ciascuno da svolgersi nel corso di una settimana.

2.5.1 Aree Tematiche e Moduli

Per l'edizione 2022 del programma sono resi disponibili le seguenti 8 *Aree tematiche:*

1. ***Introduction to Cybersecurity*** [1 Modulo]
2. ***Ethics & Soft Skills*** [1 Modulo]
3. ***Attack/Defense*** [3 Moduli]:
    - Access Control
    - Cryptographic protocols
    - Malware analysis
4. ***Cryptography*** [4 Moduli]:
    - Cryptography 0 – Background Materials
    - Cryptography 1 – Classical ciphers and symmetric-key algorithms
    - Cryptography 2 – Public-key cryptography, hashing and steganography
    - Cryptography 3 – Advanced cryptography
5. ***Hardware Security*** [4 Moduli]:
    - Hardware Security 0 – Background Materials
    - Hardware Security 1 – Introduction, Vulnerabilities due to Design bugs and flaws, Hardware Trojans
    - Hardware Security 2 – Vulnerabilities in test infrastructures and in security modules
    - Hardware Security 3 – Side Channel Attacks & Vulnerabilites in IoT
6. ***Network Security*** [4 Moduli]:
    - Network Security 0 – Background materials

- Network security 1 – Computer networks and devices
- Network security 2 – Communication Monitoring and Securing
- Network security 3 – CanBus Security

7. ***Software Security*** [4 Moduli]:
   - Software Security 0 – Program life cycle and related tools
   - Software Security 1 – Secure programming
   - Software Security 2 – Memory Corruption
   - Software Security 3 – Arbitrary Code Execution
8. ***Web Security*** [3 Moduli]:
   - Web Security 1 – Server-side vulnerabilities
   - Web Security 2 – SQL Injections and Logic Flaws
   - Web Security 3 – Client-side vulnerabilities.

La mappa concettuale che riassume le precedenze culturali tra i vari moduli è riportata in Fig. 1.

2.5.2 Organizzazione a livello di sede locale

Ciascuna sede locale è libera di organizzare liberamente il proprio percorso formativo, rispettando tuttavia i seguenti vincoli:

- Il percorso deve prevedere il completamento di almeno 12 Moduli, per un carico complessivo di didattica (frontale o remota, in funzione dei vincoli imposti dal Covid) per ciascun partecipante di 72 ore;
- Il percorso preposto deve prevedere almeno 1 modulo per ciascuna delle Aree tematiche 2÷8.

Nelle gare CTF locali e nazionali verranno proposte challenge relative alle Aree tematiche 3÷8.

2.5.3 Multidisciplinarietà

Il percorso formativo è caratterizzato da una significativa multidisciplinarietà che integra argomenti tecnici a diverso livelli di approfondimento con aspetti etici e legislativi.

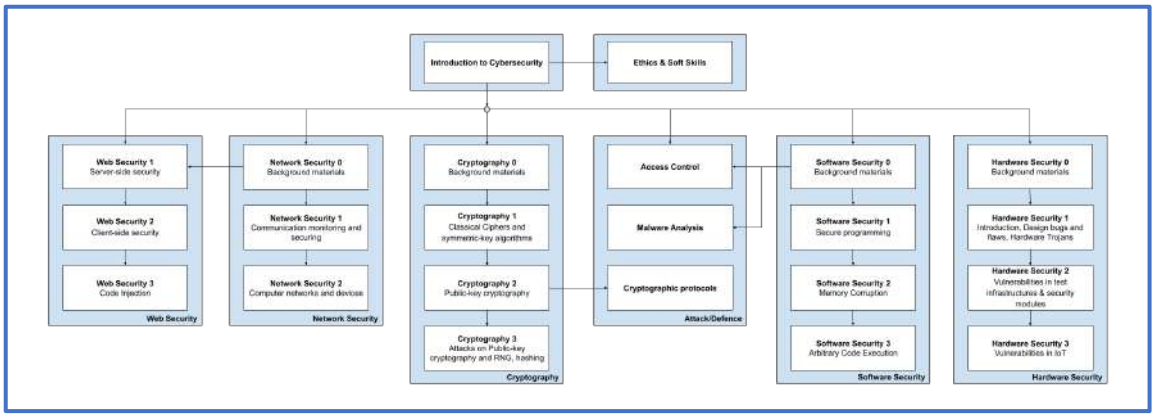

Figura 1: Mappa concettuale delle precedenze tra i vari Moduli

2.5.4 Materiale didattico

Per ciascun Modulo delle Aree tematiche 2÷8 viene reso disponibile il seguente materiale, tutto in lingua inglese:

- Prerequisiti e Learning Outcome
- Materiale propedeutico
- Tutorial sull'uso dei tool/ambienti da usarsi all'interno del Modulo
- 2 ore di lezioni teoriche, preregistrate
- Presentazione delle challenge
- Challenge da risolvere nelle 4 ore previste di Hands-on-Experience
- Challenge da risolvere come homework
- Materiale di approfondimento
- Soluzioni (write-up) delle challenge proposte (accessibili ai soli tutor).

Tutte le attività di formazione possono essere svolte in modalità remota: le relative piattaforme per l'erogazione sono rese disponibili dal Lab. Naz. Cybersecurity. L'orario delle attività didattiche è fissato liberamente da ciascuna sede.

2.6 Cronologia delle attività per l'edizione 2022

La cronologia delle attività per l'edizione 2022 è riassunta nella Tabella 1.

Tabella 1 - Cronologia dell'edizione 2022 del programma

Attività	Date
Adesione delle sedi	Entro il 02.11.2021
Adesione delle scuole superiori	Entro il 30.11.2021
Adesione delle aziende sponsor	Entro il 31.12.2021
Iscrizioni on-line	02.11.2021 - 14.01.2022
Pre-Test on-line	29.01.2022
Test di ammissione	02.02.2022
Percorso di addestramento	08.02.2022 - 28.05.2022
Gare locali (Jeopardy)	01.06.2022
Cerimonie di premiazione locali	In base alla sede
Gara Nazionale e Cerimonia di Premiazione (ILO Torino)	
○ Arrivo, apertura e demo	29.06.2022
○ *Gara nazionale (Attacco/Difesa)*	30.06.2022
○ *Presentazione dei migliori team (mattina)*	01.07.2022
○ *Recruitment Fair nazionale (mattina)*	01.07.2022
○ *Cerimonia di premiazione nazionale (pomeriggio)*	01.07.2022
○ *Social event (sera)*	01.07.2022
○ *Partenza*	02.07.2022
Ritiro della Nazionale *TeamItaly*	TBD
Campionato Europeo ECSC – Vienna	29.11.2022 - 03.12.2022
Conferenza Stampa TeamItaly	TBD

3 Edizioni passate del programma

Il programma CyberChallenge.IT è giunto alla sesta edizione. La Tabella 2 riporta l'evoluzione delle cinque edizioni precedenti e mostra che per l'edizione 2021, dopo i due test, sono stati selezionati 671 giovani tra i 4.896 inizialmente iscritti. Questi giovani hanno seguito un percorso formativo multidisciplinare, presso 31 sedi universitarie, due Accademie Militari e il C3T, distribuite sul territorio nazionale. Alla fine di tale percorso, ha avuto luogo prima una competizione locale con sfide uguali e contemporanee in tutte le sedi, e poi una gara nazionale: il quarto campionato italiano Capture-The-Flag (CTF) in cybersecurity.

Tabella 2 - Partecipanti alle precedenti edizioni del programma

Anno	Sedi	Scuole	Studenti partecipanti								
			Registrati							Ammessi	
			Totale	Genere		Provenienza					
				M	F	Scuole		Università			
			#	#	#	#	%	#	%	#	%
2017	1	-	683	603	80	57	8.3	626	91.7	20	2.9
2018	8	-	1866	1698	168	583	31.2	1283	68.8	160	8.6
2019	18	19	3203	2830	373	1341	41.9	1862	58.1	360	11.2
2020	28	114	4452	3848	604	1960	44.0	2492	56.0	560	12.5
2021	33	184	4896	4255	641	2262	46.2	2634	53.7	671	13.7

4 TeamItaly: Nazionale Italiana di Cyberdefender

Il Laboratorio Nazionale Cybersecurity ha ricevuto mandato dal Nucleo per la Sicurezza Cibernetica della Repubblica Italiana di formare una *Squadra Nazionale Italiana Cyberdefender* che rappresenti l'Italia nelle competizioni internazionali.

Della nazionale, che ha preso il nome di *TeamItaly*, vengono chiamati a far parte i ragazzi che meglio hanno dimostrato le proprie capacità, sia a livello individuale, sia come gioco di squadra, durante le varie fasi della CyberChallenge.IT.

A livello europeo ENISA, la *European Union Agency for Cybersecurity* fa da volano e, facendo tesoro delle esperienze delle singole nazioni, organizza ogni anno la *European Cyber Security Challenge* (ECSC) con lo scopo di favorire lo scambio di conoscenza e talenti su tutta Europa. La competizione è aperta a tutti i paesi europei. Ogni nazione che si iscrive all'evento partecipa con una squadra composta da 10 giocatori di un'età compresa tra i 14 e i 25 anni.

L'Italia ha partecipato, con *TeamItaly*, per la prima volta a ECSC nel 2017 conquistando il terzo posto. Nel 2018 ha ottenuto la sesta posizione, mentre nell'edizione del 2019 ha conquistato il secondo posto (Fig. 1). L'edizione 2020 non si è svolta a causa del Covid19. L'edizione 2021 della competizione si è svolta a Praga dal 28 settembre al 1° ottobre 2021 e il TeamItaly ha conquistato il terzo posto (Fig. 2).

In preparazione alla partecipazione a ogni edizione della ECSC, la squadra è chiamata a una settimana di "ritiro" in cui vengono convocati 20 ragazzi, 10 dei quali vengono successivamente selezionati per partecipare alla competizione.

Figura 1. Premiazione di TeamItaly a ECSC 2019

Figura 2: Premiazione di TeamItaly a ECSC 2021