Programma CyberChallenge.IT 2021 – *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 2021 del programma CyberChallenge.IT[1], organizzato e gestito dal Laboratorio Nazionale Cybersecurity del CINI[2].

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 dal Sistema di Informazione per la Sicurezza della Repubblica, Presidenza del Consiglio dei Ministri 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).

2.1.3 A chi è rivolto

I candidati sono giovani fra 16 e 23 anni che studiano nelle Scuole Superiori e nelle Università italiane.

Per l'edizione 2021, le iscrizioni sono aperte ai giovani nella fascia di età compresa tra i 16 e i 23 anni compiuti nel 2020, vale a dire per i nati negli anni 1997-2004; l'iscrizione è gratuita.

2.1.4 Obiettivi

Il programma vuole creare e far crescere la comunità dei cyberdefender investendo sui giovani e 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 tramite specifiche sfide che saranno chiamati ad affrontare;

[1] https://cyberchallenge.it

[2] https://cybersecnatlab.it

- 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 Superiori e nelle Università, tramite due test. Il primo viene svolto on-line da remoto e serve per una prima selezione; il secondo viene invece svolto in presenza presso le diverse università aderenti al programma e serve per formare le squadre.

Il programma di formazione affianca alla didattica tradizionale un approccio orientato alla *gamification* che si traduce nella partecipazione a competizioni in arene virtuali che simulano scenari di reti e ambienti lavorativi 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 2021, come le precedenti, offrirà agli studenti selezionati corsi di addestramento presso le sedi universitarie partecipanti e culminerà nel *quarto campionato italiano Capture-The-Flag (CTF) in cybersecurity* che permetterà di identificare la *Squadra Nazionale di Cyberdefender* che parteciperà alla European Cyber Security Challenge (ECSC)[3].

Per gli studenti delle Scuole Superiori 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 Benefici per i partecipanti

2.2.1 Benefici per gli studenti

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

- Approfondimento di argomenti di cybersecurity;
- Percorso di formazione, riconosciuto, in termini di crediti formativi, da molte Università e Scuole Superiori 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 cybersecurity 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;
- Opportunità di mettersi alla prova, misurando le proprie soft skill e attitudini, tramite l'output offerto da un *Game-based Assessment* che consentirà l'auto-valutazione, relativamente a 26 tratti di personalità e 8 abilità cognitive;

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

- Possibilità di ricevere, al termine del percorso di formazione, sia *attestati di partecipazione* rilasciati dal Laboratorio Nazionale, sia degli *Open Badge*[4], fruibili tramite la piattaforma Bestr[5] del CINECA.

2.2.2 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 offrire agli studenti coinvolti (con un piccolo investimento aggiuntivo da parte della sede) la possibilità di:
    - accedere a percorsi di "coaching", ovvero di sviluppo e crescita personale nonché professionale, che allenano lo studente al raggiungimento di obiettivi futuri:
    - conoscere linguaggi e competenze relazionali per il lavoro in team, mirando anche all'acquisizione di strumenti per raggiungere un obiettivo comune e condiviso, e ad agire come organismo unico durante le competizioni locali e nazionali attraverso la creazione di un modello di collaborazione condiviso;
- Opportunità di poter utilizzare, per l'eventuale erogazione del percorso formativo in modalità remota, di piattaforme messe a disposizione dal Lab. Naz. Cybersecurity.

[4] https://openbadges.org

[5] https://bestr.it

2.2.3 Benefici per le Scuole Superiori federate

Tra gli aspetti più rilevanti come ritorno per le Scuole Superiori partecipanti al programma vanno evidenziati:

- Iscrizione gratuita al programma, entrando ufficialmente nel Network CyberChallenge.IT;
- Possibilità di offrire agli studenti coinvolti l'opportunità di:
  - essere sensibilizzati alle problematiche di cybersecurity, e conoscere i possibili sbocchi nel mondo del lavoro,
  - incrementare la propria visibilità verso aziende e istituzioni, tramite la condivisione dei CV su una piattaforma dedicata;
  - incontrare significativi attori pubblici e privati del panorama della cybersecurity nazionale;
  - partecipare a *Percorsi per le competenze trasversali e per l'orientamento*;
  - essere convocati a far parte di TeamItaly, la Nazionale Italiana di Cyberdefender, e di partecipare anche a competizioni internazionali del settore;
  - effettuare *Stage* e *Internship* presso aziende del settore, significative istituzioni nazionali, e sedi del Laboratorio Nazionale di Cybersecurity dislocate sul territorio nazionale;
- Possibilità, per i propri docenti e studenti, di accedere gratuitamente a un ampio e approfondito materiale didattico, predisposto e rivisto da esperti;
- Possibilità, per i propri docenti, di partecipare gratuitamente a corsi mirati di introduzione e/o approfondimento su tematiche di cybersecurity.

2.2.4 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:
    - accedere gratuitamente a tutto il materiale didattico messo a disposizione dal programma;
    - 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.

2.3 Ruolo dei principali stakeholder

Il programma 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*
- *Comparto Intelligence Nazionale*
- *Ministero della Difesa*
- *Ministero dell'Istruzione*
- *Ministero dell'Università e della Ricerca*
- *Sistema Universitario Italiano*
- *Aziende private.*

In particolare, il *Laboratorio Nazionale Cybersecurity* opera da coordinatore dell'intero programma, 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 programma e 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 programma beneficia della collaborazione con il *Comparto Intelligence Nazionale* e con il *Ministero della Difesa*. Il primo considera il programma in linea con quanto previsto dal *Piano Nazionale per la protezione cibernetica e la sicurezza*, mentre il secondo contribuisce all'organizzazione della competizione finale nazionale, anche ospitandola presso proprie strutture.

Il *Ministero dell'Istruzione,* che ritiene importanti tutte quelle iniziative che puntino a incoraggiare i giovani allo studio di discipline tecnico scientifico (STEM), promuove il programma verso tutti gli istituti scolastici superiori, anche attraverso avvisi mirati, e contribuisce al supporto delle attività nell'ambito di *Percorsi per le competenze trasversali e per l'orientamento*.

Ovviamente il programma si avvale della collaborazione dei diversi attori del *Sistema Universitario Italiano*: nell'edizione 2020 sono state ben 26 le sedi universitarie che hanno aderito al programma. Le singole università utilizzano il programma 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.

In questa fase, 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, come integrazione dell'attività formativa.

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 e che 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 di programmazione ma anche senza conoscenze di cybersecurity.
   Il test di ammissione si svolge in due fasi:
   a. test on-line che, se superato, consente l'accesso al successivo, in presenza;
   b. test in presenza, svolto contemporaneamente presso tutte le sedi coinvolte, che porta all'individuazione 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 (per i dettagli si veda la sezione 2.5). Il percorso ha una durata complessiva di 72 ore distribuite su tre mesi e viene svolto in orari compatibili con le attività didattiche degli studenti.
6. Una *gara CTF locale individuale,* mirata a selezionare i migliori studenti di ciascuna sede. Presso ciascuna sede, alla gara segue una premiazione locale e una recruitment fair 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 quale 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 2021 del programma sono resi disponibili le seguenti 7 *Aree tematiche:*

1. ***Introduction to Cybersecurity*** [1 Modulo, opzionale]
2. ***Attack/Defense*** [5 Moduli]:

- Access Control
- Cryptographic protocols
- Malware analysis
- Network security 1 – Computer networks and devices
- Network security 2 – Communication Monitoring and Securing

3. ***Cryptography*** [3 Moduli]:
   - Cryptography 1 – Classical ciphers and symmetric-key algorithms
   - Cryptography 2 – Public-key cryptography, hashing and steganography
   - Cryptography 3 – Advanced cryptography
4. ***Hardware Security*** [4 Moduli (il Modulo *Hardware Security 0* è opzionale)]:
   - Hardware Security 0 – VHDL for Modeling, Simulation and Synthesis of RT- and Gate-Level Descriptions
   - Hardware Security 1 – Introduction, Design bugs and flaws, Hardware Trojans
   - Hardware Security 2 – Vulnerabilities in test infrastructures & security modules
   - Hardware Security 3 – Vulnerabilities in IoT
5. ***Software Security*** [4 Moduli (il Modulo *Software Security 0* è opzionale)]:
   - Software Security 0 – Program life cycle and related tools
   - Software Security 1 – Secure programming
   - Software Security 2 – Memory Management and Buffer overflow
   - Software Security 3 – Code reuse attacks
6. ***Web Security*** [3 Moduli]:
   - Web Security 1 – Server-side vulnerabilities
   - Web Security 2 – Client-side vulnerabilities
   - Web Security 3 – Code Injection
7. ***Ethics & Soft Skills*** [1 Modulo]

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÷7.

Nelle gare CTF locali e nazionali verranno proposte challenge relative alle Aree tematiche 2÷6.

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, legislativi e di soft skill.

Per la valutazione delle soft skill è stato scelto, a seguito di una gara pubblica, un *Game-based Assessment* che consente a ciascun partecipante di auto-valutarsi, grazie alla misurazione di diversi parametri e abilità cognitive. Al termine del percorso, ciascun partecipante riceverà direttamente un report riassuntivo, che potrà liberamente utilizzare.

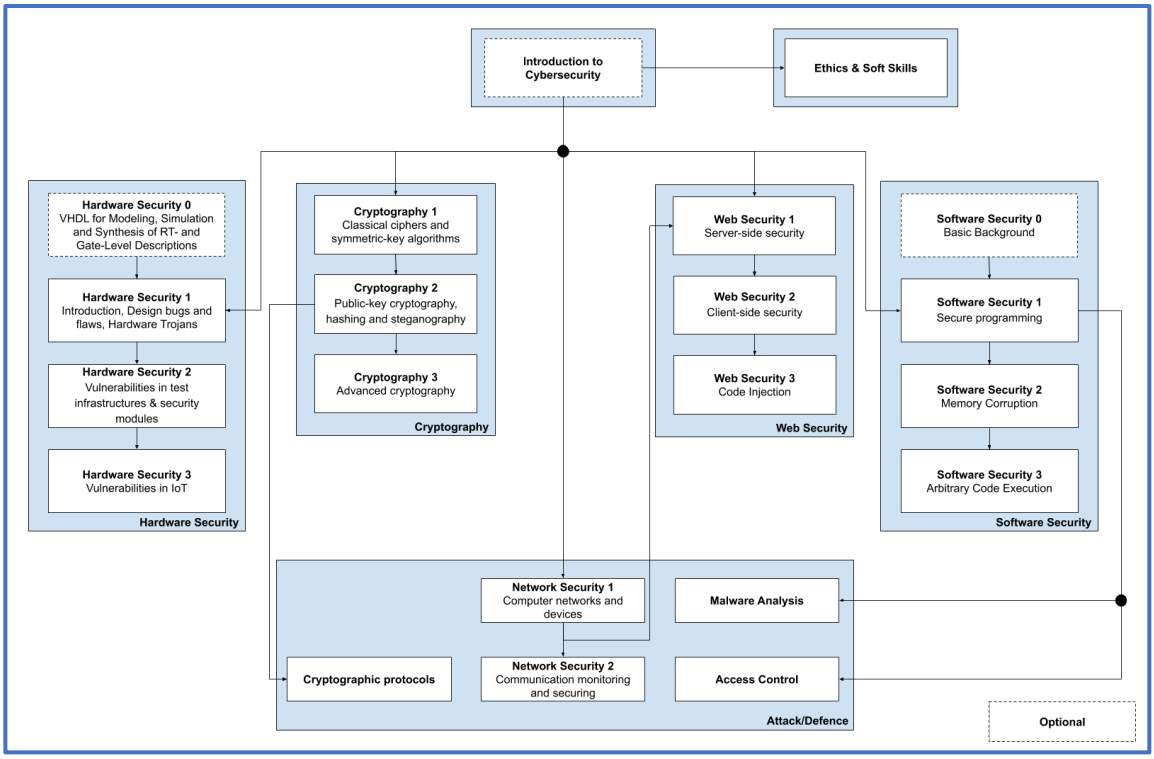

Figura 1: Mappa concettuale delle precedenze tra i vari Moduli

2.5.4 Materiale didattico

Per ciascun Modulo delle Aree tematiche 2÷6 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 2021

La cronologia delle attività per l'edizione 2021 è riassunta nella Tabella 1.

Tabella 1 - Cronologia dell'edizione 2021 del programma

Attività	Date
Adesione delle sedi	Entro il 31.10.2020
Adesione delle scuole superiori	Entro il 30.11.2020
Adesione delle aziende sponsor	Entro il 31.12.2020
Iscrizioni on-line	01.11.2020 - 17.01.2021
Pre-Test on-line	22.01.2021 - 24.01.2021
Test di ammissione	02.02.2021
Percorso formativo	08.02.2021 - 28.05.2021
Simulazione di Gara Attacco/Difesa	16.04.2021
Gare locali (Jeopardy)	03.06.2021
Cerimonie di premiazione locali	04.06.2021
Simulazione di Gara nazionale	19.06.2021
Gara nazionale (Attack/Defence)	07-08.07.2021
Recruitment Fair nazionale	08.07.2021
Cerimonia di premiazione nazionale	09.07.2021
Ritiro della Nazionale *TeamItaly*	05.09.2021 - 11.09.2021
Campionato Europeo ECSC – Praga	28.09.2021 - 01.10.2021

3 Passate edizioni del programma

Il programma CyberChallenge.IT è giunto alla quinta edizione. La Tabella 2 riporta l'evoluzione delle quattro edizioni precedenti e mostra che per l'edizione 2020, dopo i due test, sono stati selezionati 560 giovani tra i 4.452 inizialmente iscritti. Questi giovani hanno seguito un percorso formativo multidisciplinare, presso 28 sedi: 26 atenei, il *Comando per la Formazione e Scuola di Applicazione* e il *Centro di Competenza in Cybersecurity Toscano* (C3T). Alla fine di tale percorso, hanno avuto luogo prima una competizione locale con sfide uguali e contemporanee in tutte le sedi, e successivamente una gara nazionale: il terzo campionato italiano Capture-The-Flag (CTF) in cybersecurity.

Tabella 2 - Partecipanti alle precedenti edizioni del programma

Year	Training Nodes	High Schools	Involved students								
			Booked							Enrolled	
			Total	Gender		Origin					
				M	F	High Schools		Universities			
			#	#	#	#	%	#	%	#	%
2017	1	-	**683**	603	80	57	8.3	626	91.7	**20**	2.9
2018	8		**1,866**	1,698	168	583	31.2	1,283	68.8	**160**	8.6
2019	18	19	**3,203**	2,830	373	1,341	41.9	1,862	58.1	**360**	11.2
2020	27 + 1	114	**4,452**	3,848	604	1,960	44.0	2,492	56.0	**560**	12.5

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 podio, guadagnandosi il secondo posto** (Fig. 1). L'edizione 2020 non si è svolta a causa del Covid19. L'edizione 2021 della competizione si svolgerà a Praga dal 28 settembre al 1° ottobre 2021. L'Italia ospiterà la competizione nell'autunno del 2024.

In preparazione alla partecipazione a ogni edizione della ECSC, la squadra è convocata per una settimana di "ritiro".

Figura 2 : Premiazione di TeamItaly a ECSC 2019

Figura 3: Incontro di TeamItaly con il Premier Conte