CYBERSECURITY
NATIONAL
LABORATORY

consorzio
interuniversitario
nazionale
per l'informatica

TEAM ITALY
CYBERDEFENDER

OLICYBER
OLIMPIADI ITALIANE DI CYBERSICUREZZA

CYBER
TRIALS

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

TeamItaly: Nazionale italiana di Cyberdefender
Olicyber: Olimpiadi di Cybersecurity
CyberTrials

Capitolato per attività di Team Building e sviluppo di Soft Skill

Indice

1 Introduzione

Questo documento ha l'obiettivo di illustrare le seguenti esigenze:

- Attività di Team Building, in presenza, per 20 studenti selezionati per il ritiro 2022 di TeamItaly[1], la squadra nazionale di Cyberdefender
- Attività di formazione e sviluppo soft skill per studenti e studentesse delle scuole superiori secondarie che partecipano al Programma Olicyber – Olimpiadi di Cybersecurity 2022.
- Attività di formazione e sviluppo soft skills per studentesse delle scuole superiori secondarie che partecipano al Programma CyberTrials per l'edizione 2022.

2 Programma di training - TeamItaly

Il Laboratorio Nazionale di Cybersecurity del CINI, con l'obiettivo di preparare al meglio gli studenti e le studentesse alle più importanti gare internazionali del settore, in affiancamento al training sulle tematiche specialistiche, si propone di allenare e formare gli stessi al gioco di squadra, nello specifico a favorire la comunicazione e l'affiatamento tra i membri del team nell'ottica di migliorare apprendimento e passione in vista del raggiungimento di un obiettivo comune.

Il programma, che verrà replicato per l'edizione 2022, si articola nelle seguenti fasi:

- **FASE 1:**
  - Definizione di un modello che rilevi l'attitudine a specifiche competenze soft in ambito Team Building.
  - Questa prima fase dovrà:
    - Coinvolgere i 20 giovani studenti selezionati per far parte del TeamItaly, compreso il coach della squadra
    - Periodo di inizio e chiusura fase 1 da concordare con la Committenza
- **FASE 2:**
  - Due giornate di training in presenza, presso la sede nella quale si svolgerà il ritiro
  - Questa seconda fase dovrà:
    - Coinvolgere i 20 giovani studenti selezionati, compreso il coach della squadra
    - Fornire un report di dati aggregato relativo alla Fase 1
    - Periodo di inizio e chiusura fase 2 da concordare con la Committenza
- **FASE 3:**
  - Follow-up in modalità online per i soli 10 titolari scelti per le competizioni internazionali a valle del ritiro
    - Periodo di inizio e chiusura fase 3 da concordare con la Committenza
- **FASE 4:**
  - Restituzione feedback alla Committenza

Scadenza del programma: data partenza alla *European Cyber Security Challenge (*ECSC)[2] della edizione 2022.

[1] https://teamitaly.eu

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

3 Programma di training – Olicyber

Il Progetto di traning sulle Solf Skill per gli studenti e le studentesse selezionate per il programma Olicyber vuole perseguire, accanto alla formazione e training sulle materie specialistiche di settore, diversi obiettivi tra i quali:

- Sviluppare una nuova prospettiva verso la conoscenza e lo sviluppo delle soft skill, come indispensabile per la conoscenza di sé stessi e per il "successo" nella vita professionale e personale e piena realizzazione di sé;
- Identificare le proprie performance come connubio tra apprendimento continuo, crescita personale e realizzazione di sé;
- Educare al concetto di formazione continua e apprendimento delle proprie risorse e abilità personali, già in fase di adolescenza.

Il programma, che verrà replicato per l'edizione 2022, si articola nelle seguenti fasi:

- **FASE 1:**
  - Micro progettazione dell'intervento formativo (solo per la 1° edizione) e predisposizione delle classi;
  - Contattare i 100 studenti;
  - Predisposizione calendario concordato con la Committenza.
- **FASE 2:**
  - Erogazione dell'intervento formativo, con le seguenti caratteristiche:
  - Durata: totale di 40h per discente;
  - Periodo di inizio e chiusura dell'intervento da definire con la Committenza;
  - Erogazione di un percorso diviso in fasi;
  - Coinvolgimento di 100 giovani selezionati.
- **FASE 3:**
  - Valutazione dei risultati;
  - Survey dettagliata dell'impatto del training;
  - Restituzione feedback alla Committenza.

Scadenza del programma: Data delle Olimpiadi di Cybersecurity 2022.

4 Programma di training – CyberTrials

L'obiettivo di questo programma parte dall'assunto che ancora troppe ragazze e donne vivono nella "inconsapevolezza" culturale di poter contribuire nello sviluppo proprio delle materie scientifiche esattamente come i propri compagni di scuola, amici e colleghi.

Nello specifico, il progetto si pone, come obiettivo primario il facilitare la comprensione del contesto socio-culturale in cui queste giovani donne, già in età adolescenziale (14-18 anni), sono immerse, per consentire loro di vivere con maggiore consapevolezza e con minore senso di inadeguatezza le proprie prospettive di studio, di lavoro e di vita ancora troppo caratterizzate come tipicamente maschili; e quindi in particolare l'attenzione al tema della parità di contributo delle donne nei campi STEM, in egual misura degli uomini.

Il programma si svilupperà in parallelo al programma di training Olicyber.

Il programma, che verrà replicato per l'edizione 2022, si articola nelle seguenti fasi:

- **FASE 1:**
  - Micro progettazione dell'intervento formativo e predisposizione delle classi
  - Contattare le 50 studentesse
  - Predisposizione calendario concordato con la Committenza
- **FASE 2:**
  - Erogazione dell'intervento formativo per un totale di 40h
  - Erogazione di un percorso diviso in fasi
  - Coinvolgere le 50 giovani studentesse selezionate
- **FASE 3:**
  - Valutazione dei risultati
  - Survey dettagliata dell'impatto del training
  - Restituzione feedback alla Committenza

Scadenza del programma: Data delle Olimpiadi di Cybersecurity 2022

Appendice 1 - TeamItaly: Nazionale Italiana di Cyberdefender

Mission

Il *Teamitaly - la squadra Nazionale Italiana CyberDefender* - nata grazie all'esperienza formativa della CyberChallenge.IT[3], è formata da giovani talenti che meglio hanno dimostrato le proprie capacità, sia a livello individuale, sia come gioco di squadra, durante le varie fasi della CyberChallenge.IT.

L'obiettivo è quello di rappresentare l'Italia partecipando ai più importanti concorsi internazionali del settore, tra cui l'annuale European Cybersecurity Challenge (ECSC)[4].

Riconoscimenti istituzionali

Il TeamItaly 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) della Repubblica Italiana ha affidato al Laboratorio Nazionale di Cybersecurity del CINI il compito di organizzare e gestire le attività di TeamItaly e di curarne, tra l'altro, la partecipazione alle competizioni internazionali del settore.

Il ritiro della Nazionale Italiana

Per potersi preparare alle competizioni internazionali, il team è coinvolto in un percorso di addestramento intensivo (ritiro).

Durante il ritiro, in aggiunta al training sulle tematiche specialistiche, è previsto anche un percorso di Team Building specificamente progettato per l'iniziativa.

[3] https://www.cyberchallenge.it/

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

Appendice 2 - European Cyber Security Challenge (ECSC)

A livello europeo, ENISA[5], 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'European Cyber Security Challenge (ECSC),** è una competizione di cybersecurity, promossa dalla Commissione Europea e dall'agenzia europea per la sicurezza delle reti e dell'informazione (ENISA).

Il progetto si svolge all'interno delle iniziative del National Cyber Security Programme[6], per un investimento complessivo di £1.9 miliardi. Investimento considerevole, che sottolinea l'importanza e l'attenzione che tutti i paesi stanno riconoscendo e rivolgendo alla sicurezza informatica.

Tra gli obiettivi dell'ECSC vi è quello di porre la **cybersecurity a servizio dell'umanità**, per promuovere la pace, preservare la democrazia, la dignità e la libertà di pensiero, stimolando la collaborazione tra i giocatori dei paesi partecipanti alla gara e l'importanza della trasparenza e dell'osservanza delle regole per tutte le fasi della competizione.

L'ECSC include ogni anno una serie di eventi, tra cui conferenze e un recruitment fair, workshop, dimostrazioni, talk ed esposizioni di aziende attive nell'ambito della cybersecurity.

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 è svolta a Praga dal 28 settembre al 1° ottobre 2021 e il Teamitaly ha conquistato il terzo posto.

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

[5] Https://www.enisa.europa.eu/.

[6] Programma sviluppato all'interno del National Cyber Security Strategy dell'UK. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Appendice 3 – Olicyber: Olimpiadi di Cybersecurity

Mission

OliCyber.IT - Olimpiadi Italiane di Cybersicurezza è un programma di valorizzazione delle eccellenze mirato a favorire e incentivare l'avvicinamento degli studenti alle problematiche della cybersicurezza.

Il programma mira a coinvolgere i ragazzi di tutti gli anni di tutti gli istituti superiori di II grado e si avvale dell'esperienza e degli strumenti messi a punto dal Laboratorio Nazionale Cybersecurity del CINI nell'ambito del programma CyberChallenge.IT[7], al quale ragazzi e ragazze possono aderire a partire dai 16 anni. Da questo punto di vista, OliCyber.IT si pone come programma "propedeutico" a CyberChallenge.IT, che ne è visto come il naturale complemento a valle.

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.

Dal 2021 "Olicyber.it - Olimpiadi Italiane di Cybersicurezza" sono state riconosciute 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.

A chi è rivolto

Il programma mira a coinvolgere le studentesse e gli studenti iscritti a un qualsiasi istituto superiore di secondo grado, indipendentemente dall'anno frequentato.

La partecipazione al programma e alla gara finale è gratuita.

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;
- offrire ai ragazzi le conoscenze di base di necessarie a sostenere l'ammissione e la formazione al programma CyberChallenge.IT.

Metodologia e contenuti formativi

Gli studenti vengono selezionati, a seguito di informazione capillare negli istituti superiori di secondo grado tramite una prova di selezione.

[7] https://cyberchallenge.it

Il programma di competizioni affianca alle tematiche tradizionali un approccio orientato alla *gamification,* che si traduce nella partecipazione a competizioni in arene virtuali che simulano scenari di reti e ambienti reali. Il modello proposto è unico nel suo genere nel panorama internazionale.

La futura edizionei 2022 offrirà agli studenti selezionati dalla selezione scolastica e dalla selezione territoriale, sessioni di tutoraggio di addestramento online e culminerà nella *Seconda e Terza Olimpiade italiana di Cybersecurity*.

Appendice 4 – CyberTrials

Missione

Cyber Trials è un programma intensivo di formazione su temi relativi alla sicurezza informatica affrontati in chiave umanistica o comunque a basso contenuto tecnico. Il progetto nasce dall'esigenza di costruire un'offerta efficace nell'ambito della sicurezza informatica anche per quelle persone che hanno minore confidenza con I linguaggi di programmazione o l'architettura di una rete informatica. Nello specifico, la prima edizione di cyber trails si concentrerà su un target di ragazze delle scuole superiori di II grado, per incoraggiarne l'adesione agli argomenti della cybersecurity anche da un punto di vista più umanistico e accessibile senza particolari conoscenze pregresse in ambito tecnico.

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;
- Introdurre, attraverso un approccio umanistico, anche materie tecnicamente più impegnative
- Creare un viatico per rafforzare l'adesione di giovani ragazze, ancora poco coinvolte in Italia nelle materie STEM, a progetti quali Olicyber.

Metodologia e contenuti formativi

Le studentesse vengono selezionate, a seguito di informazione capillare negli istituti superiori di secondo grado, tramite una prova di selezione.

Il programma prevede la formazione e attività di apprendimento attraverso il gioco su argomenti umanistici legati al mondo della cybersicurezza, quali Osint, Socmint, Social Engineering.