



Co-funded by  
the European Union



Implemented by



## Future Minds Lab Initiative

### TERMS OF REFERENCE 81-16-25-6

#### Repeated Call

**Title: External Trainer – Vocational Training in Cybersecurity: Offensive and Defensive Operations**

**Location: Bosnia and Herzegovina**

**Level of Effort: 5 training days, 5 days of mentoring (spanning across 5 month-period) and 2 preparation days**

**Reporting to: Project Manager, Future Minds Lab Initiative**

**Type of Contract: Short-term Individual Contract**

#### 1. Background

Bosnia and Herzegovina faces a persistent shortage of skilled professionals in the field of cybersecurity and digital technologies. According to international assessments such as the OECD and UNICEF, the country suffers from limited access to digital infrastructure, low levels of digital literacy, and a mismatch between education outputs and labour market needs. This digital gap is particularly evident among youth aged 19 – 29, who often lack opportunities for structured, market-relevant training that leads directly to employment in high-demand digital sectors.

At the same time, the cybersecurity threat landscape is rapidly expanding, with businesses and public institutions increasingly exposed to risks ranging from data breaches and ransomware to advanced persistent threats. Yet, the availability of trained cybersecurity professionals in Bosnia and Herzegovina remains critically low. This skills gap not only affects the security of local enterprises but also undermines the country's overall competitiveness and resilience in the digital economy.

The Future Minds Lab (FML) Initiative, implemented by the University Sarajevo School of Science and Technology (SSST) under the SEDEP program and supported by GIZ, was established to address these challenges. The Project operates across three strategic objectives:

- Enhancing industry innovation through stronger cooperation between innovators and businesses.
- Improving the enabling environment for innovation through expert advice, targeted training, and technical assistance.
- Increasing the supply of skilled entrepreneurs and digital workers through vocational training and education.

Within this third objective, the Project supports the creation of a 6-month vocational training program designed to provide market-relevant IT skills to young people. The training focuses on three high-demand tracks: Game Design, Cybersecurity, and Cloud Computing, all identified as critical for the domestic and regional labour markets.



Co-funded by  
the European Union



Implemented by



This Call for Proposals relates to the Cybersecurity – Offensive and Defensive Operations component, designed to equip participants with hands-on skills in configuring and defending systems, identifying vulnerabilities, and mitigating attacks. Delivered through a combination of training days, mentoring sessions, and practical labs, the module prepares participants for roles in penetration testing, security engineering, and SOC environments.

## 2. Objective

To engage a qualified external trainer to deliver practical training modules in offensive and defensive cybersecurity with the goal of preparing participants to detect, analyze, and respond to security threats in real-world scenarios.

## 3. Key responsibilities

- Develop a detailed training curriculum and materials (presentations, labs, exercises) covering:
  - Configuration and testing of firewalls, IDS/IPS, and secure configurations
  - Vulnerability scanning and exploitation (Nmap, Metasploit)
  - Web and API security (OWASP Top 10, mobile application security)
  - Log analysis, SIEM tools, and security monitoring.
- Guide participants through lab-based exercises and red/blue team simulations.
- Provide mentoring sessions to support participants in completing assignments and understanding real-world application.
- Adapt teaching to varying skill levels of participants.
- Participate in progress monitoring meetings with the Project Team.
- Submit a final report (max. 3 pages) summarizing the curriculum, content delivered, participant progress, and recommendations.

## 4. Deliverables

- **Training Curriculum – Structured curriculum with learning outcomes /2 days of preparation/** (First payment: 20%)
- **Module Delivery – Facilitation of 5 one-day modules + 5 days of mentoring, total 10 days/** (Second payment: 50%)
- **Final Report – Summary of training delivered and recommendations** (Third payment: 30%)

## 5. Timeline for delivery

Deliverable	Due Date
Preparation of Training Curriculum and materials	November 24 2025
Module Delivery	November 2025 - March,
Final Report Submission	2026 March 15, 2026



Co-funded by  
the European Union



Implemented by



## 6. Qualifications

- Minimum 3 years of professional experience in network/application security, penetration testing, or working with SOC teams.
- Strong knowledge of security principles, vulnerability scanning (Nmap, Metasploit), firewalls, IDS/IPS, and SIEM monitoring.
- Ability to work with youth with mixed skill levels.
- Excellent communication and presentation skills.
- Fluency in the local language; working proficiency in English.

## 7. Application requirements

Applicants must submit:

- CV detailing relevant experience
- Short motivation letter
- Short outline of proposed training approach (one page) including methodology, structure, tools to be used and learning outcomes
- Financial offer (daily fee rate).

## 8. Selection criteria

Criterion	Weight
Professional experience in cybersecurity (offensive and defensive)	40%
Quality of proposed training approach	20%
Relevance to target group (youth, entry-level)	20%
Financial offer	20%

## 9. Language of the Assignment

Training will be conducted in the local language, while the final report must be submitted in English.

## 10. Submission Deadline

All interested candidates are to submit their bids with all supporting documents no later than November 14, 2025, 23:59. All bids are to be submitted electronically to the following email address: [info@ssst.edu.ba](mailto:info@ssst.edu.ba), with the subject line: *81-16-25-6 FML External Trainer – Cybersecurity: Offensive and Defensive Operations. Repeated Call*. Any inquiries regarding the opportunity may be directed to the same address and subject line.



Co-funded by  
the European Union



Implemented by



## Financial Proposal Form – 81-16-25-6

Name of Bidder:	[Insert Name of Bidder]	Date:	Select date
-----------------	-------------------------	-------	-------------

Bidders are required to prepare their financial proposals following the below format and submit it with the technical offer. Any financial information provided in the technical proposal shall lead to the Bidder's disqualification.

The Financial Proposal should align with the requirements in the Terms of Reference and the Bidder's Technical Proposal.

**Currency of the proposal: BAM**

**Table 1: Summary of Overall Prices**

	Amount(s)
<b>Professional Fees</b> (from Table 2)	
<b>Other Costs</b> (from Table 3)	
<b>Total Amount of Financial Proposal</b>	

**Table 2: Breakdown of Professional Fees**

Name	Position	Fee Rate <i>A</i>	No. of Days/months/ hours <i>B</i>	Total Amount <i>C=A+B</i>
In-Country				
Home Based				
<b>Subtotal Professional Fees:</b>				

**Table 3: Breakdown of Other Costs**

Description	UOM	Quantity	Unit Price	Total Amount
Local transportation costs	Lump Sum			
Out-of-Pocket Expenses				
Other Costs: (please specify)				
<b>Subtotal Other Costs:</b>				



Co-funded by  
the European Union



Implemented by



**Table 4: Breakdown of Price per Deliverable/Activity**

<b>Deliverable/ Activity description</b>	<b>Time (person days)</b>	<b>Professional Fees</b>	<b>Other Costs</b>	<b>Total</b>
Deliverable 1				
Deliverable 2				
Deliverable 3				
.....				

**Signature of authorized person:**



Co-funded by  
the European Union



Implemented by



## Inicijativa Future Minds Lab

### PROJEKTI ZADATAK 81-16-25-6

#### Ponovljeni poziv

**Naziv pozicije: Spoljni trener – stručno osposobljavanje iz cyber sigurnosti: ofanzivne i defanzivne operacije**

**Lokacija: Bosna i Hercegovina**

**Angažman: 5 dana obuke, 5 dana mentorisanja (u periodu od 5 mjeseci) i 2 dana pripreme**

**Izvršavanje: Projektni menadžer, Inicijativa Future Minds Lab**

**Vrsta ugovora: Kratkoročni angažman pojedinačnog spoljnog trenera**

### 1. Kontekst

Bosna i Hercegovina se suočava s kontinuiranim nedostatkom kvalifikovanih stručnjaka u oblasti cyber sigurnosti i digitalnih tehnologija. Prema međunarodnim procjenama (OECD, UNICEF), zemlja ima ograničen pristup digitalnoj infrastrukturi, nizak nivo digitalne pismenosti i izražen nesklad između obrazovnih programa i potreba tržišta rada. Ovaj digitalni jaz posebno pogađa mlade osobe od 19 do 29 godina, koje često nemaju priliku za strukturirane, tržišno relevantne obuke koje direktno vode do zaposlenja u sektorima s visokom potražnjom.

Istovremeno, prijetnje u oblasti cyber sigurnosti ubrzano rastu – od krađa podataka i ransomware napada do sofisticiranih trajnih prijetnji. Ipak, broj obučeni stručnjaka za cyber sigurnost u Bosni i Hercegovini ostaje kritično nizak. Ovaj nedostatak kadra ne utiče samo na sigurnost domaćih kompanija, već i na ukupnu konkurentnost i otpornost zemlje u digitalnoj ekonomiji.

Future Minds Lab (FML) Inicijativa, koju implementira Univerzitet Sarajevo School of Science and Technology (SSST) u okviru SEDEP programa i uz podršku GIZ-a, osnovana je kako bi se odgovorilo na ove izazove. Projekat djeluje kroz tri strateška cilja:

- jačanje inovacija u industriji kroz snažniju saradnju inovatora i poslovne zajednice,
- unapređenje okruženja za inovacije kroz ekspertske savjete, ciljane obuke i tehničku podršku,
- povećanje ponude mladih preduzetnika i digitalnih radnika kroz stručno osposobljavanje i obrazovanje.

U okviru trećeg cilja, Projekat razvija 6-mjesečni program stručnog osposobljavanja s ciljem da mladima pruži tržišno relevantne IT vještine. Program se fokusira na tri oblasti visoke potražnje: Game Design, Cybersecurity i Cloud Computing, prepoznate kao ključne za domaće i regionalno tržište rada.

Ovaj poziv za prijave odnosi se na komponentu Cybersecurity – ofanzivne i defanzivne operacije, koja ima za cilj da polaznike osposobi za praktičan rad na naprednim sigurnosnim zadacima. Modul se realizuje kroz kombinaciju obuke, mentorisanja i praktičnih laboratorijskih vježbi, pripremajući polaznike za uloge u penetracionom testiranju, sigurnosnom inženjeringu i SOC okruženjima.



Co-funded by  
the European Union



Implemented by



## 2. Cilj angažmana

Angažovati kvalifikovanog vanjskog trenera za obuku iz oblasti ofanzivne i defanzivne cyber sigurnosti, s ciljem da polaznici steknu znanja i vještine potrebne za detekciju, analizu i zaštitu sistema u realnim uslovima.

## 3. Ključne odgovornosti

- Razviti detaljan kurikulum obuke i materijale (prezentacije, laboratorijske vježbe, zadatke) pokrivajući:
  - o Konfiguracija i testiranje firewalls, IDS/IPS i sigurne konfiguracije,
  - o Skeniranje ranjivosti i eksploatacija (Nmap, Metasploit),
  - o Web sigurnost i API sigurnost (OWASP Top 10, mobilne aplikacije),
  - o Analizu logova, SIEM alati i sigurnosni monitoring.
- Izvoditi obuku uživo.
- Voditi polaznike kroz studije slučaja i laboratorijske vježbe i simulacije napada/odbrane.
- Mentorisati i pružiti podršku polaznicima u izvršavanju zadataka i razumijevanju praktične primjene.
- Prilagoditi podučavanje različitim nivoima znanja polaznika.
- Učestvovati u sastancima za praćenje napretka s projektnim timom.
- Dostaviti završni izvještaj (max 3 stranice) sa sažetkom sadržaja i kurikulumu, napretka polaznika i preporukama.

## 4. Rezultati angažmana (Deliverables)

- **Kurikulum obuke – strukturiran plan obuke sa definisanim ishodima učenja /2 dana pripreme/** (prva uplata – 20%)
- **Realizacija modula – 5 jednodnevnih modula i 5 dana mentorisanja /ukupno 10 dana/** (druga uplata – 50%)
- **Završni izvještaj – sažetak obuke i preporuke** (treća uplata – 30%)

## 5. Vremenski okvir isporuke

Rezultati angažmana	Rok za isporuku
Priprema kurikuluma i materijala	24. novembar 2025.
Realizacija obuke	novembar 2025. – mart 2026.
Predaja završnog izvještaja	15. mart 2026.

## 6. Kvalifikacije

- Minimalno 3 godine profesionalnog iskustva u mrežnoj i aplikativnoj sigurnosti, penetracionom testiranju ili radu sa SOC timovima.



Co-funded by  
the European Union



Implemented by



- Odlično poznavanje sigurnosnih principa, mrežne zaštite, alata za skeniranje ranjivosti (Nmap, Metasploit), te SIEM i monitoring sistema.
- Prilagoditi način rada različitim nivoima znanja polaznika.
- Odlične komunikacijske i prezentacijske vještine.
- Tečno poznavanje lokalnog jezika; sposobnost korištenja engleskog jezika u profesionalnom kontekstu.

## 7. Potrebna dokumentacija za prijavu

- CV sa relevantnim iskustvom
- Kratko motivaciono pismo
- Kratki pregled predloženog pristupa obuci (jedna stranica) uključujući metodologiju, strukturu, alate koji će se koristiti i ishode učenja
- Finansijska ponuda (cijena po danu).

## 8. Kriteriji za odabir

Kriterij	Težina
Profesionalno iskustvo u cyber sigurnosti (ofanzivne i defanzivne operacije)	40%
Kvalitet predloženog pristupa obuci	20%
Relevantnost za ciljnu grupu (mladi, početnici)	20%
Finansijska ponuda	20%

## 9. Jezik angažmana

Obuka će se izvoditi na lokalnom jeziku, dok se završni izvještaj predaje na engleskom.

## 10. Rok za prijavu

Svi zainteresirani kandidati dužni su poslati svoje prijave sa pratećom dokumentacijom najkasnije do **14. novembra 2025. godine do 23:59 sati**. Prijave se dostavljaju isključivo elektronskim putem na slijedeću e-mail adresu: *info@ssst.edu.ba*, uz napomenu u predmetu e-maila: *81-16-25-6 FML External Trainer – Cybersecurity: Offensive and Defensive Operations. Ponovljeni poziv*. Pitanja i pojašnjenja u vezi sa pozivom mogu se poslati na istu adresu i uz isti predmet emaila.



Co-funded by  
the European Union



Implemented by



## Forma finansijske ponude – 81-16-25-6

Ime ponuđača	[ime ponuđača]	Datum:	Odaberi datum
--------------	----------------	--------	---------------

Ponuđači su obavezni pripremiti svoje finansijske prijedloge prema dole navedenom formatu i dostaviti ih zajedno sa tehničkom ponudom. Svaka finansijska informacija koja bude pružena u tehničkoj ponudi rezultat će diskvalifikacijom ponuđača.

Finansijski prijedlog treba biti usklađen sa zahtjevima iz Projektnog zadatka i tehničkom ponudom ponuđača.

**Valuta ponude: KM**

**Tabela 1: Sažetak ukupnih cijena**

	Iznos(i)
Profesionalne naknade (iz Tabele 2)	
Ostali troškovi (iz Tabele 3)	
<b>Ukupni iznos finansijskog prijedloga</b>	

**Tabela 2: Raspodjela profesionalnih naknada**

Ime	Pozicija	Tarifa <i>A</i>	Broja dana/mjeseci/sati <i>B</i>	Ukupni iznos <i>C=A+B</i>
U zemlji				
Kod kuće				
<b>Podzbir profesionalnih naknada:</b>				

**Tabela 3: Raspodjela drugih troškova**

Opis	Mjera jedinice	Količina	Jedinična cijena	Ukupni iznos
Troškovi lokalnog transporta	Paušalni iznos			
Troškovi "iz džepa"				
Ostali troškovi: (molimo navedite)				
<b>Podzbir drugih troškova:</b>				



Co-funded by  
the European Union



Implemented by



**Tabela 4: Raspodjela cijene po isporuci/aktivnosti**

Isporuka/Opis aktivnosti	Vrijeme (osoba/dani)	Profesionalne naknade	Ostali troškovi	Ukupno
Isporuka 1				
Isporuka 2				
Isporuka 3				
.....				

**Potpis ovlaštene osobe:**