

FAQ OSC

Q: Care este termenul limită pentru înscrierea la Olimpiada de Securitate Cibernetică (OSC)?

Înscrierile pentru etapa județeană se pot face până pe data de 27 februarie, ora 16:00 pentru Olimpiada de Securitate Cibernetică, ce va avea loc pe data de 2 martie 2024.

Q: Când are loc Olimpiada de Securitate Cibernetică (OSC) și cât timp durează?

Olimpiada de Securitate Cibernetică (OSC) 2024 se desfășoară în două etape:

- *Etapa județeană (online): pe 2 martie 2024, cu o durată de 6 ore, având o pauză de 30 de minute după prima oră;*
- *Etapa națională (fizic, în București): în perioada 22-25 mai 2024.*

Mai multe detalii sunt disponibile în [“REGULAMENTUL SPECIFIC PRIVIND ORGANIZAREA ȘI DESFĂȘURAREA OLIMPIADEI DE SECURITATE CIBERNETICĂ ÎN ANUL ȘCOLAR 2023 - 2024”](#)

Q: Cine stabilește subiectele pentru OSC?

Subiectele și metodologia competiției sunt elaborate și evaluate de Comisia Centrală a Olimpiadei de Securitate Cibernetică (CCOSC), formată din reprezentanți ai Directoratului Național de Securitate Cibernetică (DNSC), ai Centrului Național Cyberint din cadrul Serviciului Român de Informații, ai Asociației Naționale pentru Securitatea Sistemelor Informatice (ANSSI), precum și profesori și experți din partea partenerilor din mediul privat, Orange România și Bit Sentinel, ce vin cu o vastă experiență în organizarea de competiții de securitate cibernetică.

Q: Ce este Romanian Cyber Security Challenge (RoCSC) și care este diferența dintre RoCSC și OSC?

Despre RoCSC

Romanian Cyber Security Challenge (RoCSC) sau Campionatul Național de Securitate Cibernetică este cel mai important concurs de securitate cibernetică pentru tineri cu vârsta de până în 25 de ani.

RoCSC se organizează la nivel național și are rolul de a identifica și selecționa lotul național preliminar din care se selectează echipa României care participă la Campionatul European de Securitate Cibernetică (ECSC). Echipa națională de securitate cibernetică (Team România) va fi alcătuită din zece membri titulari (juniori - sub 21 de ani și seniori - 21 - 25 de ani), plus 2 (două) rezerve.

La RoCSC pot participa tineri din trei categorii:

- *Juniori (până în 20 ani);*
- *Seniori (21 - 25 de ani);*

- **Open** (disponibil, indiferent de vârstă), pentru entuziaștii care vor să-și testeze cunoștințele de securitate cibernetică într-un cadru competițional.

RoCSC are două faze:

- faza online, de calificări;
- faza finală, format fizic, în București.

Despre Olimpiada de Securitate Cibernetică (OSC)

Olimpiada de Securitate Cibernetică (OSC) face parte din acest an din calendarul competițiilor naționale aprobate de Ministerul Educației și este organizată de Comisia Centrală a Olimpiadei de Securitate Cibernetică (CCOSC), formată din reprezentanți ai Directoratului Național de Securitate Cibernetică (DNSC), ai Centrului Național Cyberint din cadrul Serviciului Român de Informații, ai Asociației Naționale pentru Securitatea Sistemelor Informatice (ANSSI), precum și profesori și experți din partea partenerilor din mediul privat, Orange România și Bit Sentinel, ce vin cu o vastă experiență în organizarea de competiții de securitate cibernetică.

La Olimpiada de Securitate Cibernetică (OSC) pot participa doar elevi de liceu din România.

OSC are două faze:

- etapa județeană, online
- etapa națională, format fizic, în București

Calendarul comun OSC și RoCSC pentru anul 2024

Cele două competiții se derulează în mod independent, inclusiv clasamentele participanților. Cu toate acestea, o parte dintre activități se întâmplă în același timp și cu aceleași categorii de exerciții, ceea ce reprezintă un avantaj, participanții putând concura la ambele competiții simultan.

- faza județeană OSC: online, 2 martie 2024, în paralel cu etapa de calificări a RoCSC 2024, ce se desfășoară în perioada 2-3 martie 2024;
- faza națională OSC: 22-25 mai 2024, în paralel cu etapa finală a RoCSC 2024;
- RoCSC 2024 - Bootcamp (format fizic): vară 2024 (se vor califica tineri selecționați din rândul finaliștilor RoCSC 2024 și OSC 2024, în ordinea punctajului obținut).
- ECSC 2024 - Finala (format fizic, Torino, Italia): 08 - 11 octombrie 2024 (lotul național va fi selecționat în Bootcamp și va fi format din 10 persoane + 2 rezerve)

Q: Dacă mă înscriu la OSC, dar nu mă calific în faza națională, mai pot participa la RoCSC?

Dacă un elev a ratat participarea la etapa județeană OSC sau nu s-a calificat în etapa națională OSC, își poate încerca șansa mai departe și prin intermediul calificărilor din RoCSC (2-3 martie 2024).

Q: Cine poate participa la OSC? Există o limită de vârstă?

Înscrierile sunt deschise pentru toți elevii de liceu din România.

Dacă nu mai ești la liceu și dorești să-ți testezi cunoștințele de securitate cibernetică, ai posibilitatea de a participa la RoCSC, la una dintre categoriile:

- **Juniori** (până în 20 ani);
- **Seniori** (21 - 25 de ani);
- **Open** (disponibil, indiferent de vârstă), pentru entuziaștii care vor să-și testeze cunoștințele într-un cadru competițional.

Mai multe detalii despre RoCSC [aici](#).

Q: Unde mă pot înscrie la OSC?

Înscrierile se fac exclusiv prin platforma concursului, la adresa: <https://oscj24.cyber-edu.co/>

Q: Cum se realizează evaluarea participanților?

Rezultatele concurenților vor fi disponibile în timp real, pe tot parcursul concursului, în fiecare etapă, pe platforma oficială a competiției. Ierarhia se va stabili în ordinea descrescătoare a punctajelor obținute de fiecare concurent.

Clasamentul final va fi comunicat și publicat pe site-ul rocsc.ro, în pagina dedicată, după rezolvarea contestațiilor.

Platforma de evaluare și modul de punctare

Etapa județeană/a Municipiului București și etapa națională vor fi organizate pe platforma cyberedu.ro.

#	Participant	Total Score	SLA	Offensive Points Gained	Offensive Points Lost	Defensive Points Gained	Defensive Points Lost	Stolen Rags	Lost Rags
1		100	100 SLA	10 points	0 points	10 points	0 points	10 rag	0 rag
2		100	100 SLA	0 points	0 points	10 points	0 points	10 rag	0 rag
3		100	100 SLA	0 points	0 points	10 points	0 points	10 rag	0 rag

CCOSC va comunica din timp paginile unde fiecare candidat trebuie să se înscrie. Este încurajată înscrierea elevilor din timp pe platforma cyberedu.ro și rezolvarea exercițiilor din Arhiva Educațională, pentru familiarizarea cu aceste tipuri de probleme.

Înainte de fiecare etapă, pe pagina concursului, vor fi comunicate resurse și materiale suplimentare care vor ghida participanții și le vor oferi acces la infrastructura de competiție.

Modul de punctare pentru exercițiile teoretice și cele tip “Jeopardy”

Modalitatea de calcul pentru punctele alocate fiecărui exercițiu de tip “Jeopardy” sau teoretic este anunțată înainte de rezolvarea acestuia și poate fi de două feluri:

Punctaj fix

Fiecare întrebare are un număr exact de puncte, cunoscut în avans.

Punctaj dinamic

Fiecare întrebare are un punctaj fix inițial, iar valoarea răspunsului corect scade odată cu numărul de rezolvări ale aceluși exercițiu pentru toți jucătorii, după formula:

```
scorExercitiu = min(
    max(valoareInitiala * 0.1, valoareInitiala - ((valoareInitiala /
    numarMaximJucatori) * totalRezolvari)),
    valoareInitiala
)
```

unde:

- **valoareinitiala** este totalul de puncte inițiale pentru fiecare exercițiu; în general este 500 de puncte, dar poate să difere de la un exercițiu la altul;
- **numarMaximJucatori** este numărul maxim de jucători care trebuie să rezolve un exercițiu pentru a atinge valoarea minimă și este stabilit de CCOSC înainte de etapa de concurs;
- **totalRezolvari** este numărul total de jucători care au rezolvat un exercițiu.

Un exercițiu poate avea una sau mai multe întrebări.

Modul de punctare pentru exercițiile teoretice și cele tip “Atac și Apărare” (“Attack & Defence”)

În cazul unui exercițiu de tip “Atac și Apărare”, participantul câștigă puncte pentru că atacă cu succes serviciile altor participanți și capturează steaguri pe care le trimite către platforma cyberedu.ro, își protejează propria mașină, potențial susceptibilă la aceleași vulnerabilități și se asigură că toate serviciile sale rămân operaționale. Scorul total este suma punctajelor individuale pentru fiecare serviciu.

Punctajul general

Scorul per serviciu este format din trei componente:

- **Ofensivă (Offense):** Puncte pentru steaguri capturate de la alți participanți și transmise sistemului de punctaj în perioada care rămâne valabilă.

- **Apărare (Defense):** Puncte pentru steaguri capturate de alți participanți.
- **Disponibilitate (SLA):** % pentru disponibilitatea și comportamentul corect al serviciilor participanților.

Punctajul va fi atribuit într-o manieră dinamică, pentru a armoniza scorurile pe baza participanților care au un decalaj mare de scor. Valorile ofensive și defensive vor contribui fiecare la scorul total (valoarea ofensivă fiind pozitivă și valoarea defensivă fiind negativă), iar SLA va fi utilizat ca multiplicator în scorul fiecărui serviciu.

Pentru fiecare participant, tabloul de bord va enumera punctajul total. De asemenea, va afișa pentru fiecare serviciu și va raporta procentul de SLA, scorul concurentului, numărul total de puncte câștigate și pierdute și numărul total de steaguri cucerite și pierdute.

Formula de scor - Capturarea unui steag (flag)

Conform formulei următoare, participantul care capturează un steag (atacatorul) va primi `attacker_points`, în timp ce participantul de la care este capturat un steag (victima) va pierde `victim_points`, atunci când o semnalizare este trimisă de către atacator.

```
harness = 50 * sqrt(10)
norm = ln(ln(10)) / 12

attacker_points = scale / (1 + exp((sqrt(attackService.Score)-
sqrt(victimService.Score))*norm))
victim_points = min(victimService.Score, attacker_points)

stolen_points[attacker_id][service_id][flag_id] += attacker_points
lost_points[victim_id][service_id][flag_id] -= victim_points
```

Formula de scor - Scorul total al serviciului

```
# initial score for a flag
score[participant][service][flag_id] = 1000 #this can change

# update after each flag lost/stolen
score[participant][service][flag_id] += stolen_points[participant][service][flag_id]
score[participant][service][flag_id] -= lost_points[participant][service][flag_id]

# include sla

for flag_id in services[service].totalFlags:
    sla = ticks_up[participant][service][flag_id] *
```

```
ticks_total[participant][service][flag_id]
total_service_score[participant][service] += score[participant][service][flag_id] *
sla
```

Formula de notare - Scorul total al participantului

```
total_score[participant] = 0
for service_score in total_service_score[participant]:
    total_score[participant] += service_score
```

Alte observații

- *SLA % nu se adaugă la scorul final, dar este un factor de multiplicare al scorului total.*
- *Participanții vor avea mai multe puncte, atunci când capturează steaguri de la participanții cu un scor de serviciu mai mare.*
- *Participanții vor câștiga mai puține puncte, atunci când capturează steaguri de la participanții cu un scor de serviciu mai scăzut.*

Q: Ce este un concurs de tip “Capture the Flag” (CTF)?

În securitatea informatică, concursurile de tip “Capture the Flag” reprezintă un exercițiu în care participanții încearcă să găsească șiruri de text, numite „steaguri” sau “flags”, care sunt ascunse în secret în programe, fișiere sau aplicații vulnerabile. Prin utilizarea unor tehnici specifice din domeniul securității cibernetice, un participant poate recupera steagurile și le poate valida pe platforma concursului pentru a primi punctele pentru acea probă.

Q: Ce este un exercițiu de tip “Jeopardy”?

Fiecare exercițiu este construit astfel încât, după ce este rezolvat, să ofere o soluție de tip “steag” (“flag”) care va trebui trimisă platformei pe care se organizează concursul.

Q: Ce este un exercițiu de tip “Attack & Defence (Atac și apărare)”?

În exercițiile de “Attack & Defence”, fiecare participant primește acces la unul sau mai multe sisteme informatice ce conțin vulnerabilități sau sunt configurate greșit. Obiectivele principale sunt:

- *apărarea propriului sistem;*
- *identificarea problemelor de securitate și remedierea acestora;*
- *dezvoltarea unor scripturi sau programe informatice sau utilizarea unor unelte sau tehnici specifice cu care să se conecteze la sistemele celorlalți participanți și, prin vulnerabilități nerezolvate, să extragă steagurile de pe sistemele acestora.*

În cazul exercițiilor de “Attack & Defence”, participanții primesc puncte pentru extragerea de steaguri, pentru cât timp sistemul a rezistat împotriva atacurilor, dar și pentru metodele de protecție folosite.

Q: Unde mă pot pregăti sau exersa?

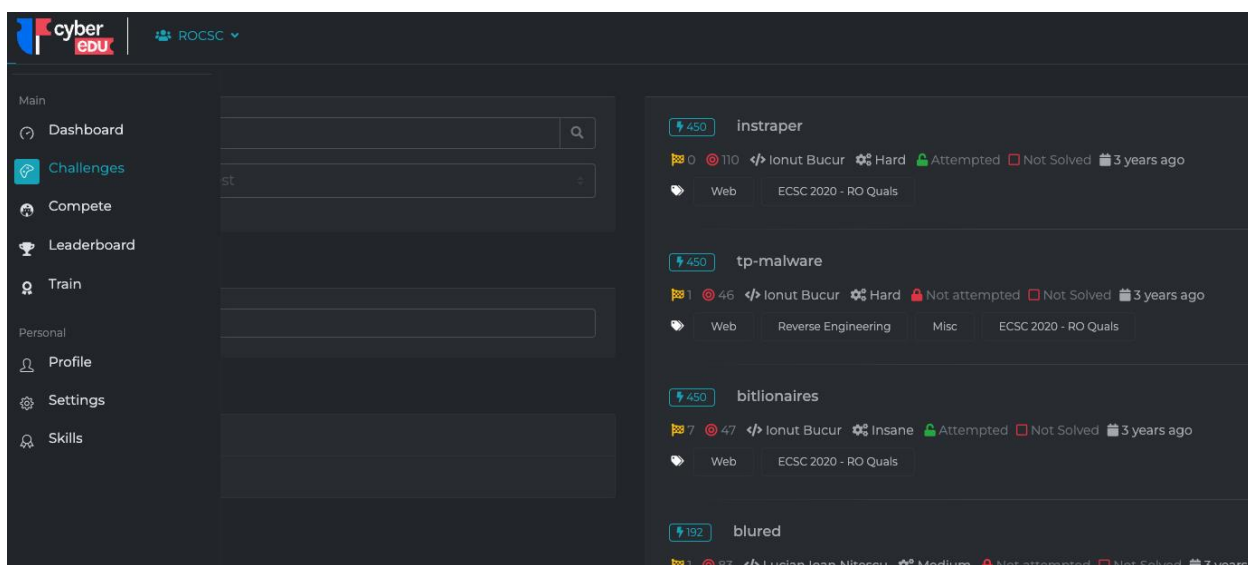
Te poți pregăti pe platforma educațională cyberedu.ro, dezvoltată de Bit Sentinel și susținută de Orange. Aceasta este platforma utilizată în toate etapele Olimpiadei de Securitate Cibernetică (OSC), pentru Campionatul Național de Securitate Cibernetică (ROCSC), dar și pentru selecționarea lotului național ce va reprezenta România la Campionatul European de Securitate Cibernetică (ECSC).

Pentru elevii cu experiență în concursuri și exerciții de tip “Capture the Flag” (CTF)

Elevii cu experiență în concursuri și exerciții de tip Capture the Flag se pot pregăti în secțiunea RoCSC de pe platforma cyberedu.ro, accesibilă prin înregistrarea unui cont. În această secțiune sunt disponibile majoritatea exercițiilor de la edițiile anterioare RoCSC (faza națională și etapa de calificări), OSC și ECSC 2019.

Pași pentru înregistrare

1. Elevul se înscrie pe pagina de înregistrare de pe site-ul cyberedu.ro.
2. Primește un email pentru confirmarea contului.
3. După validarea contului, accesează [acest link](#).
4. După accesarea link-ului de la pasul 3, obține acces la secțiunea RoCSC, iar exercițiile de la edițiile anterioare devin vizibile în secțiunea [Challenges](#) - ca în fotografia de mai jos.

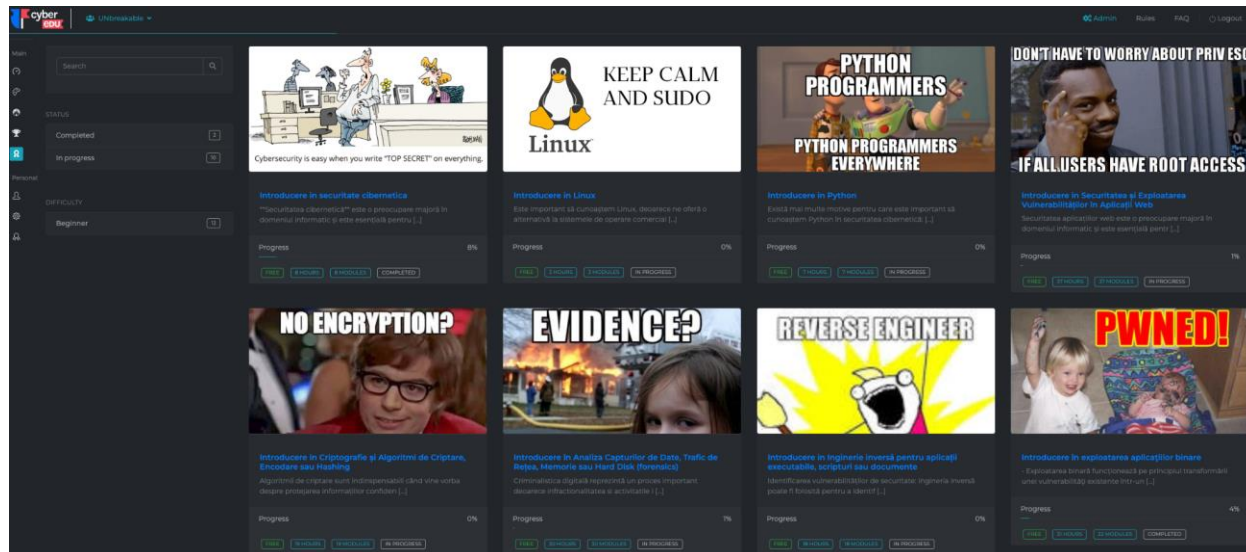


Fotografie din spațiul RoCSC de pe site-ul cyberedu.ro

Pentru elevii fără sau cu puțină experiență în concursuri și exerciții de tip “Capture the Flag” (CTF)

Elevii fără sau cu puțină experiență în concursuri și exerciții de tip “Capture the Flag”, precum și cei care își doresc o revizuire a cunoștințelor, se pot pregăti în secțiunea UNR 24/7/365, de pe platforma cyberedu.ro, accesibilă prin înregistrarea unui cont.

UNR 24/7/365 este un beneficiu în cadrul **UNbreakable România**, program implementat de Bit Sentinel și Orange România cu scopul de a-i susține pe liceenii și studenții care doresc să își construiască o carieră în domeniul securității cibernetice sau să își perfecționeze cunoștințele în domeniu. Pe platformă, elevii primesc acces la aproape 200 de exerciții rezolvate de la toate competițiile anterioare UNbreakable România, dar și la alte resurse teoretice. Evenimentele și activitățile UNbreakable se adresează în special începătorilor. Cu toate acestea, competițiile pot avea un nivel de dificultate variat, de la nivel “începător” până la “avansat”, fiind o oportunitate excelentă de pregătire pentru OSC.



Fotografie din spațiul UNR 24/7/365 de pe site-ul cyberedu.ro

Pentru a obține acces la acest spațiu există două metode:

1. Cu ajutorul unui profesor din liceul tău (metoda recomandată)

- a. Verifică dacă liceul tău este înscris în programul UNR 24/7/365, [aici](#).
- b. Dacă liceul tău este înscris:
 - i. Trimite un mesaj persoanei de contact menționată în “LISTA DE LICEE ȘI UNIVERSITĂȚI ÎNREGISTRATE ÎN PROGRAM”.
 - ii. Vei primi un mesaj cu instrucțiuni din partea persoanei de contact despre cum poți accesa secțiunea UNR 24/7/365.
- c. Dacă liceul tău nu este înscris:

- i. *la legătura cu profesorul tău de informatică sau orice persoană de decizie din liceu.*
- ii. *Trimite-i [acest link](#) în care este descris UNR 24/7/365 și [acest formular](#) pe care trebuie să-l completeze pentru a fi înrolat.*
- iii. *După ce este înrolată, persoana de contact va primi toate instrucțiunile necesare.*

2. În perioada fiecărui sezon UNbreakable România

- a. *În primăvară, de obicei în perioada februarie - mai, se organizează fiecare sezon UNbreakable România.*
- b. *În această perioadă, secțiunea UNR 24/7/365 devine disponibilă pentru cei care se înscriu în etapa de pregătire (Bootcamp) a UNbreakable România.*
- c. *Pentru înregistrarea în etapa de pregătire (Bootcamp) a UNbreakable România trebuie monitorizat site-ul oficial unbreakable.ro.*

Q: Cum pot organiza o simulare a OSC?

Pe platforma CyberEDU poți organiza propriul concurs de tip Jeopardy Capture the Flag cu exercițiile de la evenimentele anterioare ale RoCSC.

Există doar câțiva pași care trebuie parcurși pentru a programa evenimentul:

1. Welcome (Bine ai venit) - *Jucătorul înțelege beneficiile și limitările. Există câteva limitări pentru a preveni abuzul acestei funcții, care includ:*

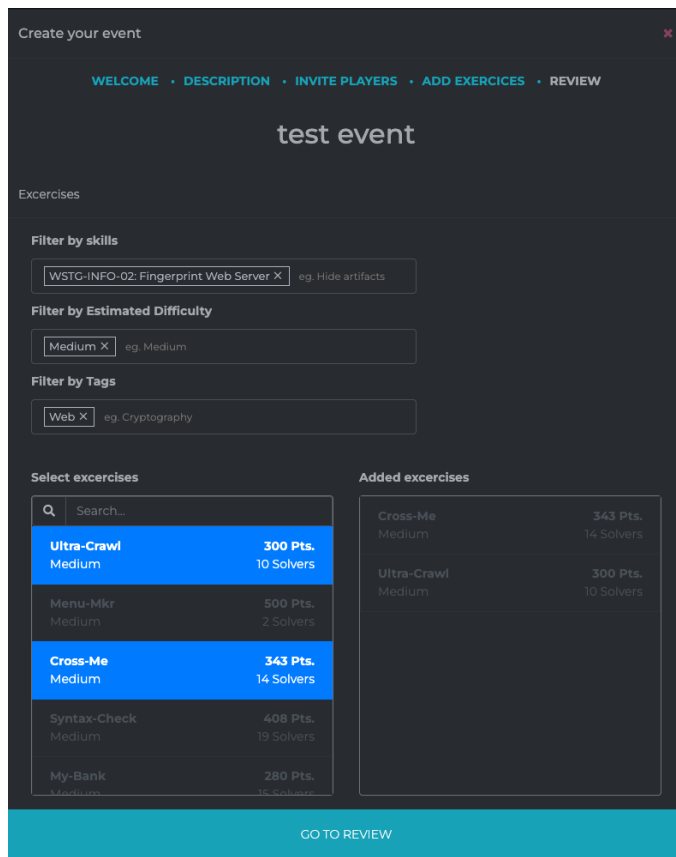
- *Maximum 8 ore pentru fiecare eveniment;*
- *Maximum 3 evenimente comunitare în același timp;*
- *Maximum 15 jucători;*
- *Evenimentele pot fi publice sau protejate prin parolă;*
- *Maximum 5 exerciții pe eveniment;*
- *Maximum un eveniment programat per organizator în același timp;*
- *Unele dintre funcții pot fi dezactivate; de ex.: vor fi statistici limitate.*

După ce jucătorul este de acord cu acești termeni și condiții, poate trece la secțiunea următoare.

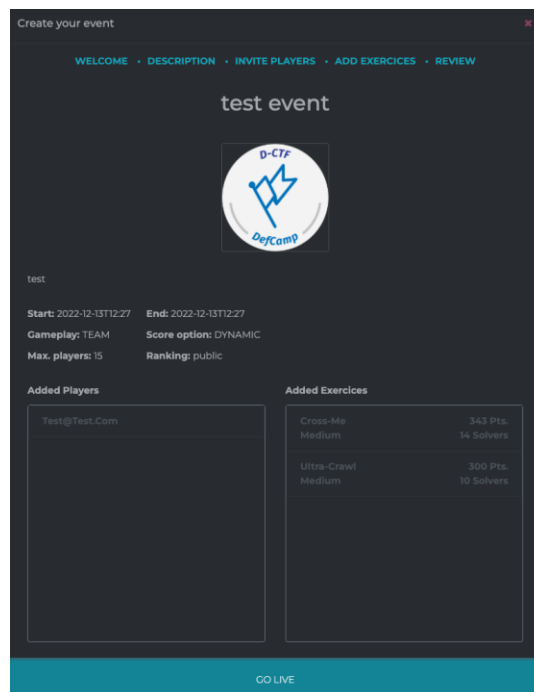
2. Description (Descriere) - *configurează câteva informații generale despre competiție. În această secțiune, un jucător poate specifica unele dintre setări, cum ar fi titlul, descrierea, data de început și de sfârșit, modul de joc (individual sau bazat pe echipă), scor (scor dinamic - la OSC se folosește scor dinamic sau static), numărul maxim de jucători, înregistrarea (publică sau protejată prin parolă) și poza pentru eveniment.*

3. Invite players (Invită jucători) - trimite o notificare prietenilor și colegilor

4. Add Exercises (Adaugă exerciții) - specifică ce provocări vor fi disponibile pentru acest eveniment. Organizatorul le poate filtra după “Aptitudini (Skills)”, “Dificultate Estimată” și “Etichete (Tags)”. Făcând click pe orice exercițiu din secțiunea „Selectați exerciții (Select Exercises)”, exercițiul va fi inclus în lista organizatorului, numită „Exerciții adăugate (Added Exercises)”.



5. Review & Publish (Revizuire și publicare). Când organizatorul este gata, poate revizui toate setările și poate lansa evenimentul. Acest eveniment va apărea în secțiunea Upcoming / Live -> Evenimente ale comunității.



Q: Din ce teme vor fi exercițiile?

Programa pentru liceu (clasele IX-XII)

Pentru faza județeană

Concepte fundamentale

Exercițiile sunt întrebări cu una sau mai multe variante de răspuns și sunt organizate sub forma unui concurs de tip “Capture the Flag”.

- *Concepte fundamentale de securitate cibernetică*
- *Tehnologii pentru asigurarea securității ciberneticice*
- *Tehnologii pentru identificarea vulnerabilităților*
- *Tehnologii de anonimizare*
- *Tehnici de inginerie socială*
- *Securitatea și managementul parolelor*
- *Participarea la programe de tip bug bounty*
- *Dezvoltarea unui business sau start-up în securitate cibernetică*
- *Concepte fundamentale de guvernanță, managementul riscului și complianță*

Exerciții practice

Exercițiile sunt de tip “Jeopardy” și vor avea un nivel de dificultate clasificat ca “ușor” sau “mediu”.

- *Criptografie și algoritmi de criptare, encodare sau hashing*
- *Securitatea și exploatarea vulnerabilităților în aplicații web*
- *Securitatea și exploatarea vulnerabilităților în aplicații mobile/desktop*
- *Informațiile obținute pe baza tehnicilor și uneltelor de tip OSINT (Open Source Intelligence)*
- *Enumerarea și exploatarea serviciilor și sistemelor*
- *Analiza jurnalelor electronice (logs)*
- *Analiza traficului de rețea*
- *Analiza capturilor de date, memorie sau hard disk (forensics)*
- *Inginerie inversă pentru aplicații executabile, scripturi sau documente*
- *Securitatea rețelelor wireless*
- *Auditul codului sursă*
- *Configurarea și securitatea sistemelor de operare și rețele*
- *Programare și scripting pentru automatizarea rezolvării unor exerciții*

Pentru faza națională

Exerciții practice

Exercițiile sunt de tip “Jeopardy” și de tip “Attack & Defence”. Acestea vor avea un nivel de dificultate clasificat ca “mediu” sau “ridicat” și sunt organizate sub forma unui concurs de tip “Capture the Flag”.

- Criptografie și algoritmi de criptare, encodare sau hashing
- Securitatea și exploatarea vulnerabilităților în aplicații web
- Securitatea și exploatarea vulnerabilităților în aplicații mobile/desktop
- Informațiile obținute pe baza tehnicilor și uneltelor de tip OSINT (Open Source Intelligence)
- Enumerarea și exploatarea serviciilor și sistemelor
- Analiza jurnalelor electronice (logs)
- Analiza traficului de rețea
- Analiza capturilor de date, memorie sau hard disk (forensics)
- Inginerie inversă pentru aplicații executabile, scripturi sau documente
- Securitatea rețelelor wireless
- Auditul codului sursă
- Configurarea și securitatea sistemelor de operare și rețele
- Programare și scripting pentru automatizarea rezolvării unor exerciții
- Cunoștințe specifice pentru exercițiile de Attack & Defence:
 - Dezvoltarea unor mecanisme de apărare a unui sistem sau rețele informatice
 - Monitorizarea unui sistem sau a unei rețele informatice pentru identificarea elementelor de securitate cibernetică
 - Identificarea și exploatarea unor vulnerabilități în sisteme informatice

Q: Care sunt avantajele participării la Olimpiada de Securitate Cibernetică și care este diferența față de Olimpiada de informatică?

Conform Wikipedia, **Olimpiada Națională de Informatică (ONI)** este o competiție anuală, în cadrul căreia concurează individual elevi din clasele V-XII.

Concursul se desfășoară în două zile și constă din două probe practice. Durata fiecăreia dintre cele două probe de concurs este anunțată în prealabil și este, de regulă, de 3-5 ore. O probă de concurs constă în rezolvarea a 1-4 probleme de natură algoritmică cu ajutorul calculatorului. Rezolvarea unei probleme presupune elaborarea unui program eficient din punct de vedere computațional, în limbajele C, C++ sau Pascal.

Pentru a se califica la faza națională, elevii trebuie să treacă înainte cu succes etapele pe școală, pe oraș și pe județ. Doar primii elevi calificați la faza județeană se califică pentru faza națională.

Olimpiada de Securitate Cibernetică, aflată la prima ediție, este organizată de Comisia Centrală a Olimpiadei de Securitate Cibernetică (CCOSC), formată din reprezentanți ai Directoratului Național de Securitate Cibernetică (DNSC), ai Centrului Național Cyberint din cadrul Serviciului Român de Informații, ai Asociației Naționale pentru Securitatea Sistemelor Informatice (ANSSI), precum și profesori și alți experți din partea partenerilor din mediul privat, Orange România și Bit Sentinel, ce vin cu o vastă experiență în organizarea competițiilor de securitate cibernetică. Membrii acestei comisii organizează evenimente, exerciții și concursuri de securitate cibernetică de peste 10 ani.

Olimpiada de Securitate Cibernetică (OSC) tratează teme dintre cele mai variate, de la securitatea aplicațiilor web până la programare sau securitatea sistemelor de operare și a aplicațiilor mobile.

Dacă Olimpiada de Informatică creează premisele unei gândiri sănătoase în programare și IT în general, Olimpiada de Securitate Cibernetică pregătește elevii pentru o carieră responsabilă în acest domeniu.