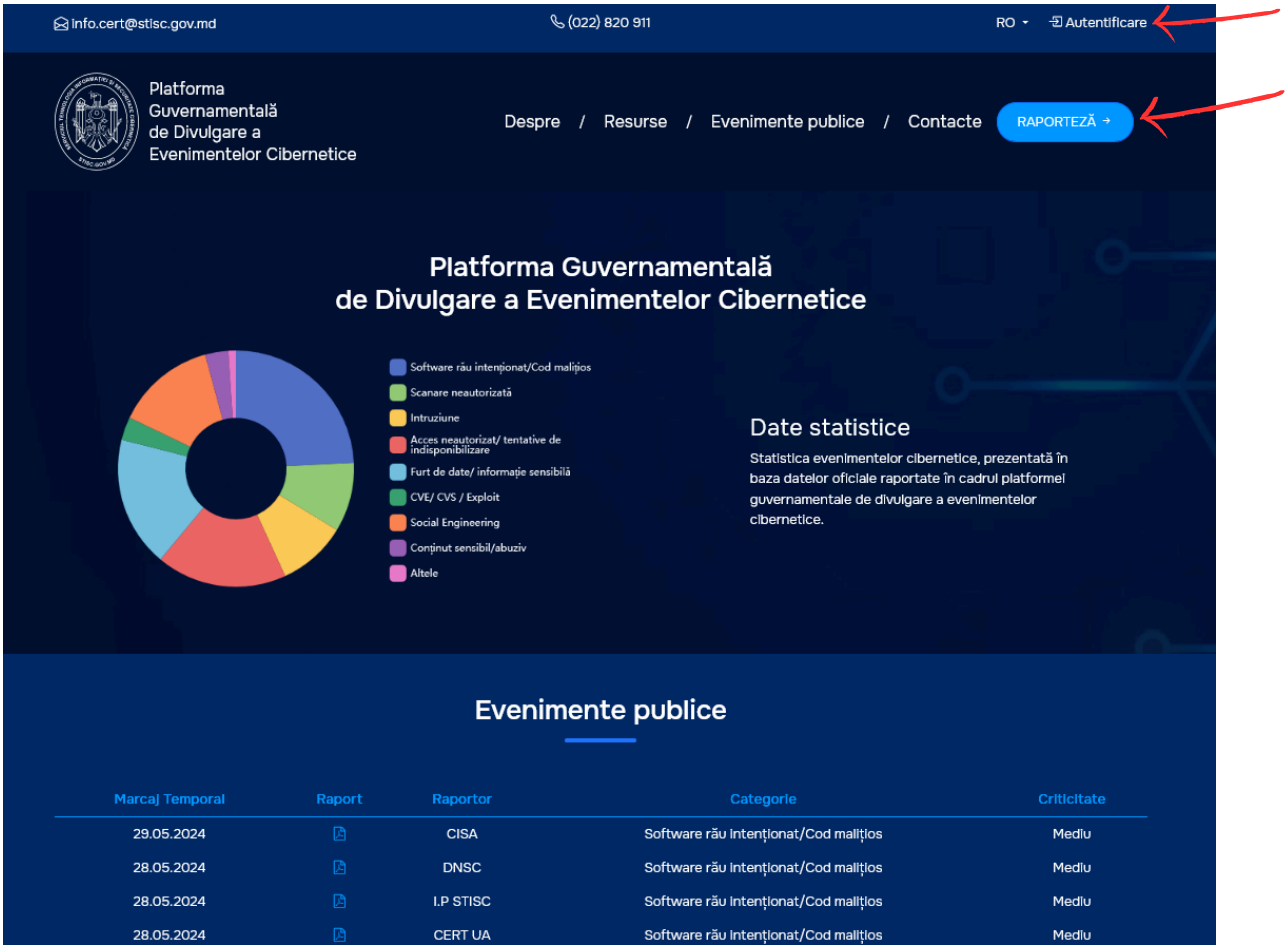
Ghid de înregistrare și de raportare eveniment cibernetic

I. Înregistrare cont utilizator

Pasul 1

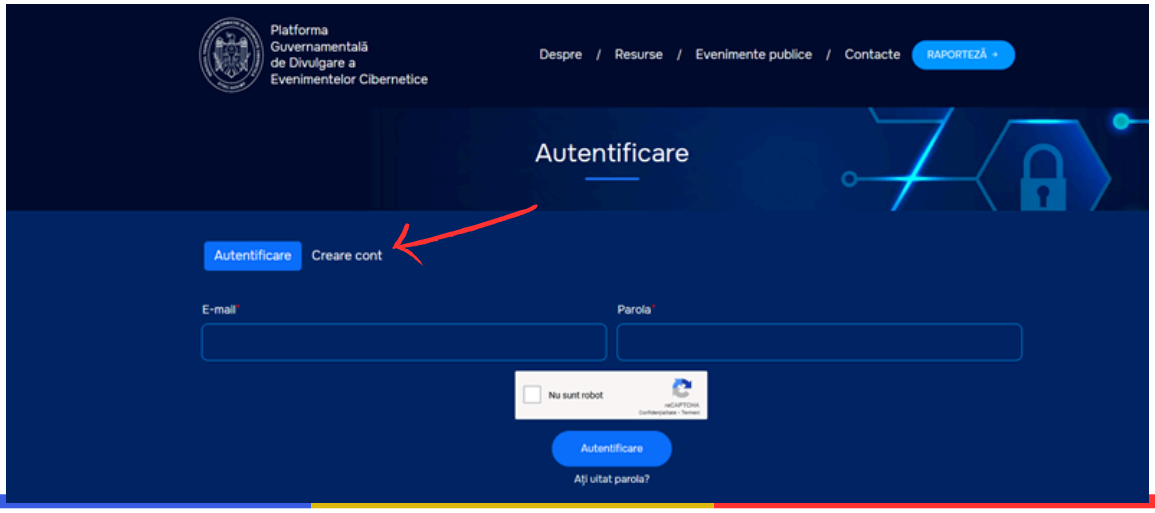
La accesare ***cyberevent.gov.md***

Accesați secțiunea AUTENTIFICARE sau butonul RAPORTEAZĂ

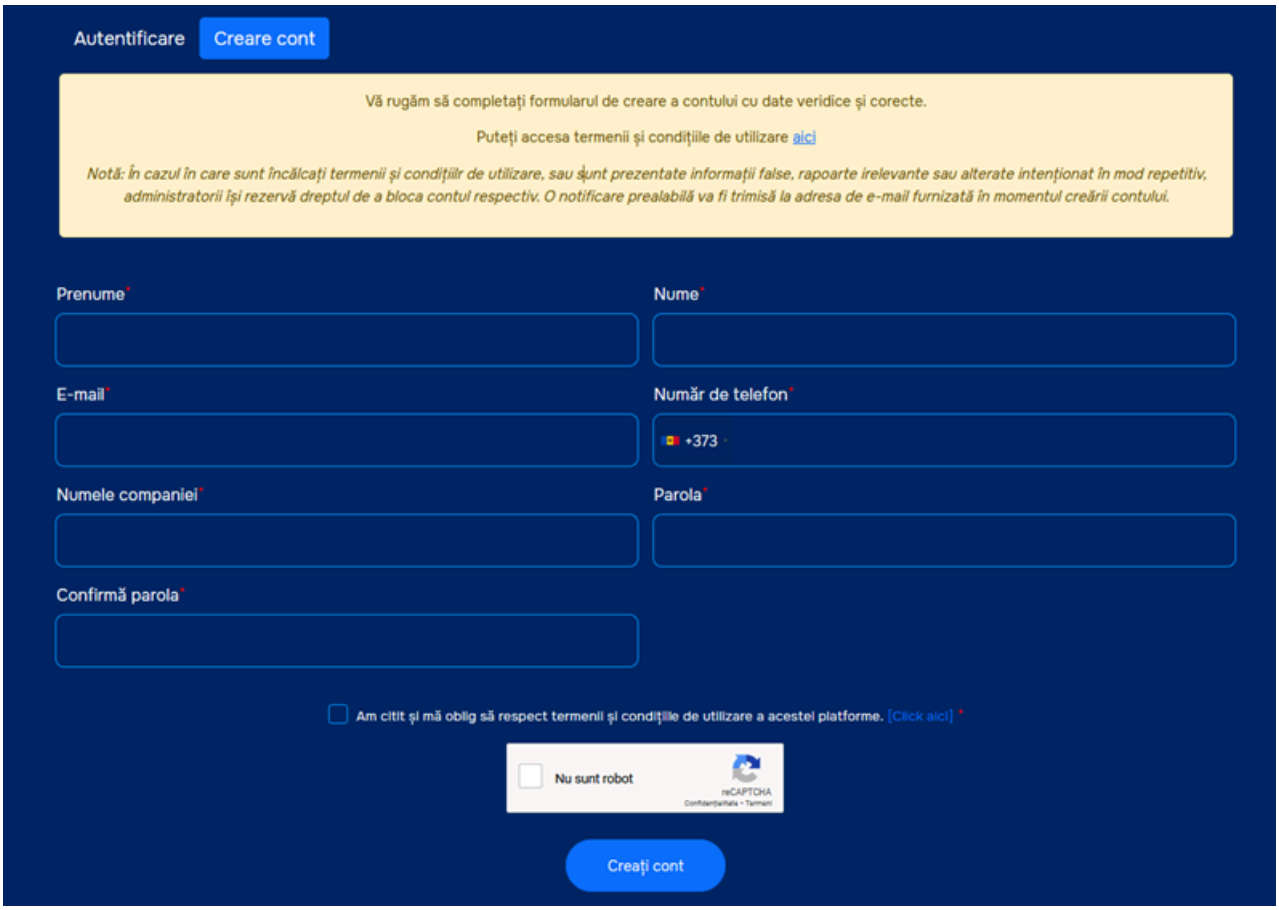


Pasul 2

Selectați *Creare cont* și completați informațiile de contact



1. Completați formularul de înregistrare, conform solicitării;
2. Asigurați-vă că parola respectă cerințele de securitate specificate de platformă;
3. Confirmați detaliile furnizate și acceptați ***Termenii și Condițiile*** serviciului.



Pasul 3

1. Verificați adresa de e-mail pe care ați furnizat-o pentru un mesaj de confirmare.
2. Accesați e-mailul și urmați link-ul de confirmare sau instrucțiunile specifice pentru a valida adresa de e-mail.
3. Asigurați-vă că informațiile dvs. sunt precise și actualizate.

Pasul 4

1. După finalizarea procesului de înregistrare, veți fi redirecționat către pagina principală.
2. Utilizați adresa de e-mail și parola pentru a vă autentifica pe platformă.
3. Acum sunteți gata să începeți utilizarea platformei.

II. Completare Raport Eveniment Cibernetic

Scopul raportării

Completați acest formular pentru a transmite către CERT Gov datele necesare identificării unui potențial atac cibernetic. Scopul este limitarea prejudiciilor și gestionarea răspunsului adecvat. Respectarea obligației legale de raportare a incidentelor cibernetice, conform Legii 48/2023, este esențială.

Completarea formularului are ca scop principal transmiterea către CERT Gov a datelor necesare identificării unui potențial atac cibernetic în vederea limitării eventualelor prejudicii și a dimensionării răspunsului necesar. Raportarea în cadrul platformei este benevolă și nu absolvește raportatorul de la obligația legală de raportare incidente cibernetice, prevăzută în Legea 48/2023.

Datele din cadrul platformei sunt tratate cu confidențialitate și securitate maximă.
Informațiile sunt înregistrate și analizate de către CERT Gov pentru identificarea și evaluarea riscurilor și amenințărilor cibernetice.

IMPORTANT! Pentru a permite distribuirea rapoartelor de analiză către alți utilizatori ai platformei web, la rubrica EVENIMENTE PUBLICE vă rugăm să bifați caseta de mai jos.

Totodată, ținem să informăm că aceasta platformă **NU este destinată raportării cazurilor de fraudă sau crimă informatică.** Dacă considerați depistarea unei infracțiuni informatice, ca urmare a analizei efectuată de Dvs, STISC recomandă sesizarea organelor de drept competente și solicitarea asistenței mutuale în prevenirea și combaterea criminalității informatice, în vederea protecției și acordării ajutorului utilizatorului sistemului informatic. Informați Poliția la numărul de telefon 112.

În cazul în care nu bifați opțiunea, evenimentul va fi analizat, însă raportul final va fi accesibil exclusiv pentru CERT Gov și Dvs., în calitate de raportor.

☐ Sunt de acord ca informațiile tehnice a evenimentului raportat să fie plasate public pentru diseminarea cunoștințelor în cadrul comunității și învățarea post-eveniment.

Categorie*

-- Nu a fost selectat --

Selectați una din categoriile disponibile, iar în cazul în care nu sunteți sigur de răspuns, alegeți categoria "Altele".

Data detectării*

31.05.2024 10:06

Indicați orientativ ziua/ora detectării evenimentului

Resursele/sistemele afectate (e-mailul compromis, adresa URL țintă atac)

Ce sisteme/resurse au fost ținta atacului (IP adresa țintă).

Descriere eveniment*

Descrieți în limbaj natural cazul identificat precum și orice detalii tehnice pe care le-ați observat.

Raportor

STISC

Instituția sau numele raportorului indicat, care va fi vizibil public.

Încărcare fișiere*

Click sau trageți fișierele aici pentru a le încărca

Puteți încărca toate informațiile colectate relaționate cu evenimentul (ex. capture de ecran, log-uri de sistem, fișierele sau atașamentele dubioase).
În format doar .zip/.pdf, mărimea maximă totală 100 MB.

Confidențialitate și securitate

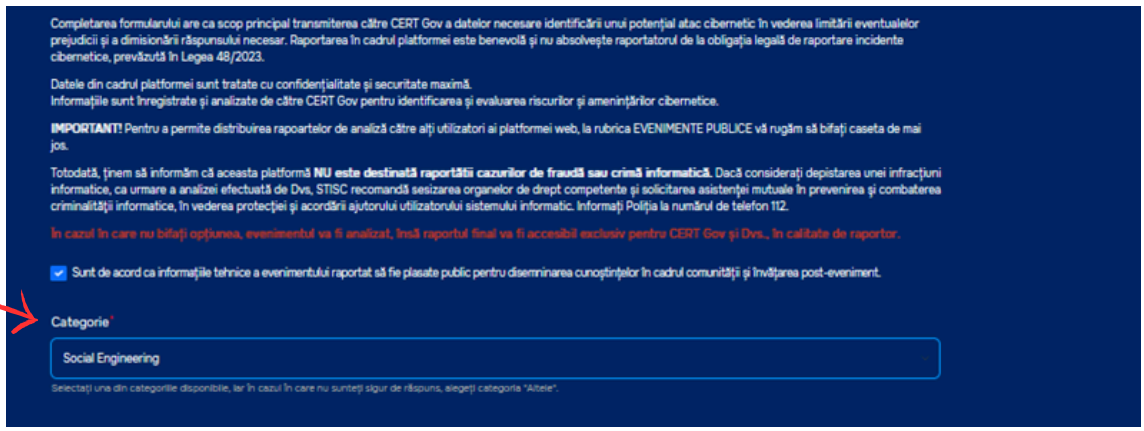
Datele furnizate sunt tratate cu maximă confidențialitate și securitate. CERT Gov analizează informațiile pentru identificarea și evaluarea riscurilor și amenințărilor cibernetice.

Evenimente Publice:

Opțional, puteți bifa o casetă pentru a permite distribuirea rapoartelor de analiză către alți utilizatori ai platformei web.

Categorizarea Evenimentului:

Selectați categoria relevantă sau "Altele" în caz de incertitudine.



1. **Data Detectării:** Furnizați data și ora detectării evenimentului.
2. **Resursele/Sistemele Afectate:** Specificați sistemele sau resursele afectate, cum ar fi adresa URL țintă sau adresa IP.
3. **Descriere Eveniment:** Descrieți evenimentul în limbaj natural și includeți detalii tehnice observate.

Informații despre raportor:
Furnizați informații despre instituție sau numele raportorului.

Încărcarea fișierelor:
Încărcați orice informații relevante legate de eveniment, cum ar fi capturi de ecran, log-uri de sistem sau fișiere dubioase. Fișierele trebuie să fie în format .zip/.pdf, cu o dimensiune totală maximă de 100 MB.

Confirmare și Acord:
Citind și acceptând termenii și condițiile de utilizare a platformei, confirmați că sunteți de acord cu respectarea acestora.

Sper că acest ghid și exemplu vă vor ajuta să completați raportul de eveniment cibernetic în mod eficient și în conformitate cu cerințele specificate.

Final

După completarea raportului veți primi notificare mail și la fel veți putea vedea statul acestui raport în cabinetul personal