



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

Info.cert@stisc.gov.md (022) 820 911 RO Autentificare

Platforma Guvernamentală de Divulgare a Evenimentelor Cibernetice

Despre / Resurse / Evenimente publice / Contacte RAPORTEAZĂ +

Platforma Guvernamentală de Divulgare a Evenimentelor Cibernetice

- Software rău intenționat/Cod malițios
- Scanare neautorizată
- Intruziune
- Acces neautorizat/ tentative de indisponibilizare
- Furt de date/ informație sensibilă
- CVE/ CVS / Exploit
- Social Engineering
- Conținut sensibil/abuziv
- Altele

Date statistice

Statistica evenimentelor cibernetice, prezentată în baza datelor oficiale raportate în cadrul platformei guvernamentale de divulgare a evenimentelor cibernetice.

Evenimente publice

Marcaj Temporal	Raport	Raportor	Categorii	Criticitate
29.05.2024		CISA	Software rău intenționat/Cod malițios	Mediu
28.05.2024		DNSC	Software rău intenționat/Cod malițios	Mediu
28.05.2024		I.P STISC	Software rău intenționat/Cod malițios	Mediu
28.05.2024		CERT UA	Software rău intenționat/Cod malițios	Mediu

Pasul 2

Selectați *Creare cont* și completați informațiile de contact

Platforma Guvernamentală de Divulgare a Evenimentelor Cibernetice

Despre / Resurse / Evenimente publice / Contacte RAPORTEAZĂ +

Autentificare

Autentificare Creare cont

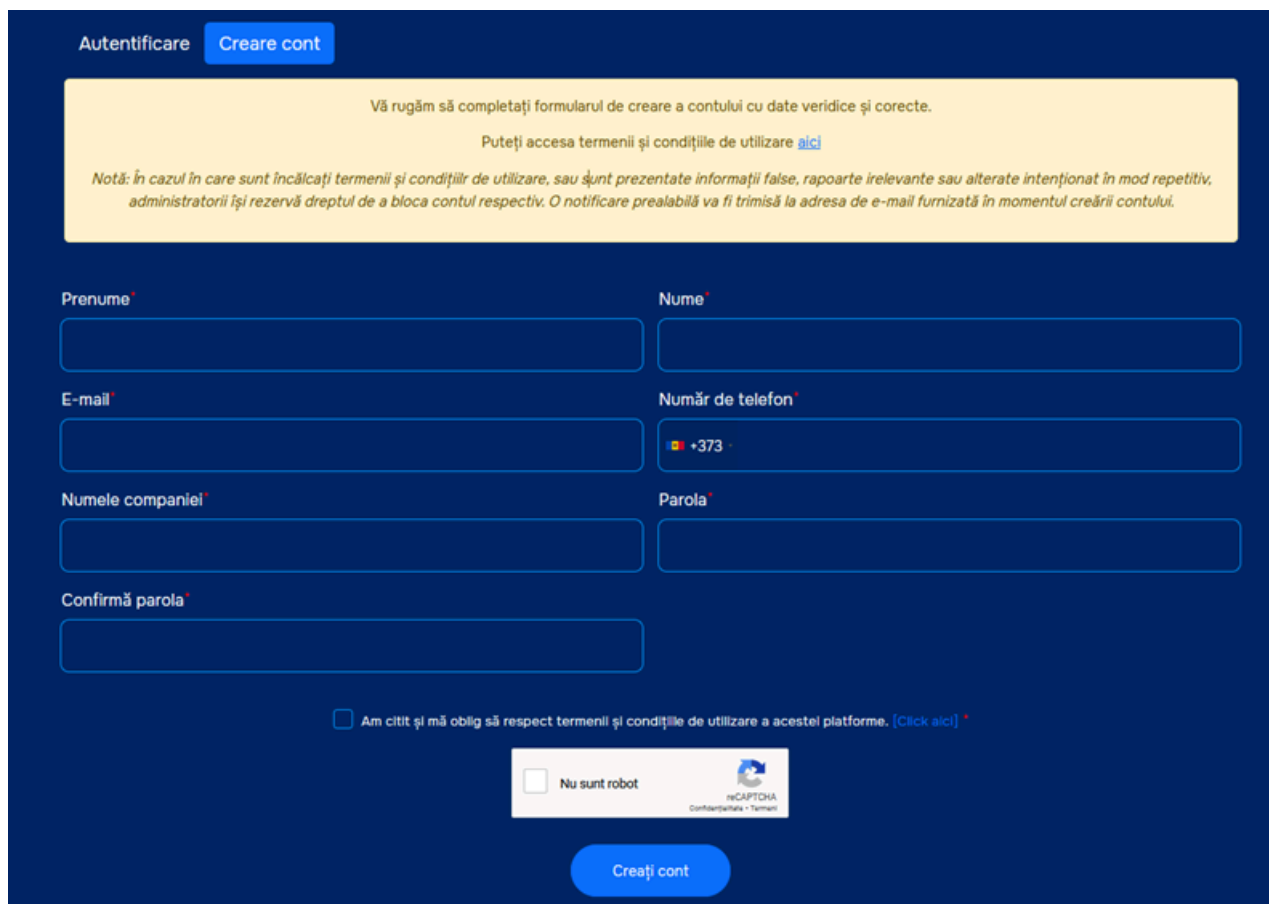
E-mail Parola

☐ Nu sunt robot

Autentificare

Ai uitat parola?

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.



The screenshot shows a web form for account creation on a dark blue background. At the top, there are two buttons: 'Autentificare' and 'Creare cont'. Below them is a yellow box with instructions: 'Vă rugăm să completați formularul de creare a contului cu date veridice și corecte.' and 'Puteți accesa termenii și condițiile de utilizare [aici](#)'. A note below states: 'Notă: În cazul în care sunt încălcați termenii și condițiile de utilizare, sau sunt prezentate informații false, rapoarte irelevante sau alterate intenționat în mod repetitiv, administratorii își rezervă dreptul de a bloca contul respectiv. O notificare prealabilă va fi trimisă la adresa de e-mail furnizată în momentul creării contului.'

The form fields are arranged in two columns:

- Left column: 'Prenume*' (text input), 'E-mail*' (text input), 'Numele companiei*' (text input), and 'Confirmă parola*' (text input).
- Right column: 'Nume*' (text input), 'Număr de telefon*' (text input with a dropdown for country code, currently showing '+373'), and 'Parola*' (password input).

Below the fields, there is a checkbox labeled 'Am citit și mă oblig să respect termenii și condițiile de utilizare a acestei platforme. (Click aici)'. Below that is a reCAPTCHA widget with the text 'Nu sunt robot' and the reCAPTCHA logo. At the bottom, there is a blue button labeled 'Creați cont'.

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 redirectionat 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 ciberneticе, 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 dimisionării răspunsului necesar. Raportarea în cadrul platformei este benevolă și nu absolvește raportatorul de la obligația legală de raportare incidente ciberneticе, 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 ciberneticе.

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 competentă 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 relevante cu evenimentul (ex. capture de ecran, log-uri de sistem, fișiere sau etapele dubioase).
În format doar .zip/.pdf, mărimea maximă totală 100 MB.

Confidențialitate și securitate

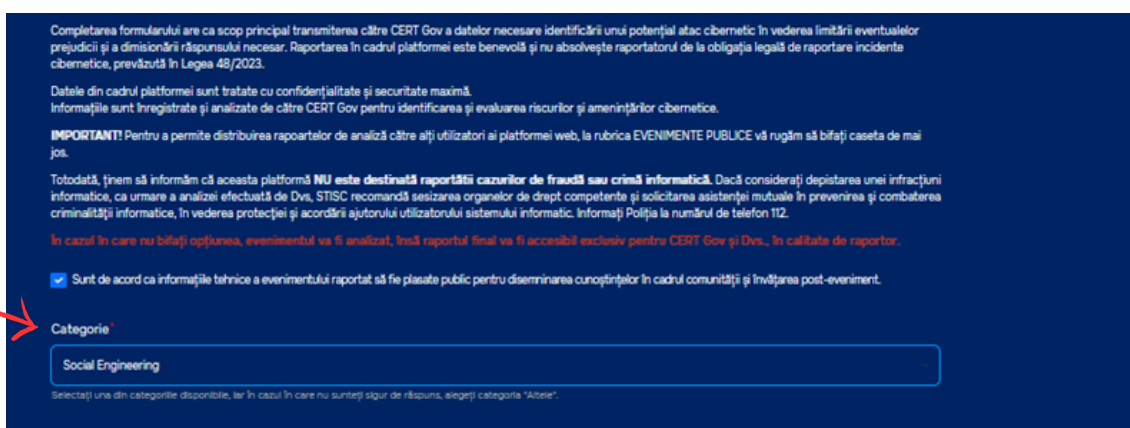
Datele furnizate sunt tratate cu maximă confidențialitate și securitate. CERT Gov analizează informațiile pentru identificarea și evaluarea riscurilor și amenințărilor cibernetice.

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.



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 dimisionării 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 această 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 competentă 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

Social Engineering

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

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.



Data detectării

31.05.2024 13:02

Indicați orientativ ziua/ora detectării evenimentului

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

E-mailul instituțional compromis TEST@TEST.GOV.RO URL-TEST.GOV.RO

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

Descriere eveniment

Un utilizator a primit un e-mail phishing cu un link suspect. Link-ul a condus către o pagină web falsă care încerca să obțină informații de autentificare.

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

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.

Raportor

STISC

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

Încărcare fișiere *

0.3 MB
sample.pdf
Elimină

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

☒ Am citit și mă oblig să respect termenii și condițiile de utilizare a acestei platforme. [\[Click aici\]](#) *

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

Rapoarțele mele						
Marșaj Temporal	Starea cazului	Categorie	Resursele/sistemele afectate	Criticitate	Raport	
31.05.2024	Înregistrat	Social Engineering	E-mailul instituțional compromis TEST@TEST.GOV.MD URL: TEST.GOV.MD	-	-	