DIRECTORATUL NATIONAL
DE SECURITATE CIBERNETICA

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SECURITATE CIBERNETICĂ ÎN INSTITUȚIILE PUBLICE

- **Conformitate NIS2 – Q & A**
- **Prezentarea soluției SIEMBIOT - Demo**

10 Decembrie 2025

DIRECTORATUL NATIONAL
DE SECURITATE CIBERNETICA

SIEMBIOT®

Powered by expertware

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Situația actuală și tendințe globale

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2021

CNA Financial:
Au plătit 40 mil $

2021

Acer :
(REvil) cere
100 mil $

2021

UK Royal Mail (LockBit)
80 de mil $

2022

Companie Fortune 50 plată de 75 mil $ către grupul Dark Angels.

2024

Duvel Moortgat
Producția oprită 3 zile la fabricile de bere din BE și US

2025

Administrația Francofona Belgia:
Afectate toate aplicațiile serviciului public folosite de cetățeni

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Incidente în servicii critice

Land Rover – Incident cibernetic (sep 2025)

Impact: Atac ransomware care a vizat serverele critice Land Rover, blocând accesul la date operaționale și criptând fișiere esențiale pentru gestionarea comenzilor și pieselor auto.

Efecte: Linia de producție oprită 2 luni, daune financiare de peste **1bil BP**, întârzieri în procesarea comenzilor și reparațiilor, iar unele operațiuni au fost nevoite să fie realizate manual, afectând lanțul de servicii post-vânzare.

Orange Romania (feb 2025)

Impact: Atacatorii au reușit să extragă 6,7 GB de date, după ce au compromis datele de acces (nume utilizator și parola) pentru o aplicație internă.

Efecte: Au fost extrase date cu caracter personal ale unor clienți și angajaților.

26 Spitale din Romania (feb 2024)

Impact: Atac cibernetic masiv de tip ransomware asupra serverelor de producţie pe care rulează sistemul informatic HIS. Ca efect al atacului, sistemul este nefuncţional, fişierele şi bazele de date sunt criptate.

Efecte: Servicii medicale paralizate, pacienți care așteaptă la camera de gardă.

Electrica (dec 2024)

Impact: DNSC a oferit suport în remedierea problemei şi investigarea incidentului, unul de tip ransomware.

Efecte: Sisteme interne au fost afectate dar sistemele critice pentru alimentarea cu curent electric nu au fost afectate.

Source: https://siembiot.eu/cyber-security-news?orderBy=date_desc&pageSize=20&pageNumber=1&searchText=ransomware

La nivel mondial au loc aproximativ 1,7 milioane de atacuri pe zi.

85% dintre companii au fost vizate de cel puțin un atac cibernetic în decursul unui an.

Fraudele informatice din România au crescut cu 40,2% în 2024.

În România, sunt detectate între 20.000 și 30.000 de atacuri cibernetice zilnic.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tendințe și metode folosite de atacatori:

2025: Phishing-ul a rămas foarte răspândit (16% dintre breșe), iar atacurile API/aplicații publice au persistat. Colectarea acreditărilor, ransomware-ul și malware-ul — în special cele care folosesc software comercial pentru persistență — domină

2025: Costul mediu al încălcării ransomware/extorcare a ajuns la 5,08 milioane de dolari. Costul mediu al breșei în SUA a atins însă 10,22 milioane de dolari, un record istoric.

2025: Sectoarele industrial, de sănătate și de servicii pentru consumatori au rămas ținte principale ale ransomware-ului. Atacurile IoT au avut o medie de 820.000 pe zi la nivel mondial

2025: Activitatea a crescut în rândul grupurilor afiliate Chinei și Iranului, precum și în rândul noilor actori ransomware (renașterea Cl0p, dominația RansomHub, noii veniți Funksec, Vanhelsing, Babuk 2.0). Crima organizată s-a adaptat, folosind adesea instrumente de furt de acreditări bazate pe AI.

2024: Vectorii comuni au inclus phishing (cel mai frecvent), utilizarea conturilor valide (31% în sectoarele critice) și exploatări ale aplicațiilor publice (26%).

2024: Costul mediu global al breșei a fost de aproximativ 4,88 milioane de dolari, iar sectoarele din sănătate și SUA sunt mult mai mari

2024: Breșele de securitate au crescut cu 75% de la an la an, cu o medie de 1.876 de atacuri per organizație pe trimestru. Atacurile DDoS au crescut cu 46% față de anul precedent

2024: Grupuri notabile au inclus rusești (de exemplu, Midnight Blizzard/Nobelium), nord-coreene și sindicate criminale motivate financiar care foloseau ransomware ca armă principală.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tendințe și metode actuale folosite de atacatori:

2025: Numărul de noi vulnerabilități estimat la 41.000–50.000, atacatorii folosind automatizarea și inteligența artificială pentru exploatare aproape imediată după dezvăluire; Timpul de exploatare tinde spre ore sau zile după publicare.

2025: Timpul de identificare a scăzut la 181 de zile; Ciclul de detecție al atacurilor este de 241 de zile— atacatorii pot funcționa în **continuare luni de zile** pe sistemele dumneavoastră fără să fie detectați.

2025: Sindicate de criminalitate cibernetică: RansomHub (cel mai activ), Cl0p (renaștere), cu grupuri noi precum Funksec și Vanhelsing; Eliminările forțelor de ordine au atenuat, dar nu au oprit proliferarea grupurilor.

Actorii folosesc acum instrumente avansate pentru a pătrunde chiar și în cele mai bine protejate sisteme:

- Utilizarea inteligenței artificiale pentru automatizarea atacurilor
- Inginerie socială avansată, inclusiv “phishing” personalizat și “deepfake-uri”.
- Atacuri de tip “ransomware” care criptează datele și blochează operațiunile.
- Atacuri către furnizorii de servicii IT
- Atacuri asupra dispozitivelor IoT, ca puncte de intrare în rețelele organizaționale
- Persistență pe termen lung în rețele compromise.
- “Infostealrs” exploatează vulnerabilitățile navigatoarelor Internet pentru a colecta parole.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Metodele de atac cele mai răspândite

Tipuri de impact

- Întreruperea activității
- Furt de date
- Acces neautorizat

• Atacuri DDoS

- Activitate maximă în aprilie 2024, cu atacuri susținute de volum foarte mare, depășind **10.000 Mbps**
- Preponderent generate de grupări hacktiviste, vizând disponibilitatea serviciilor de online banking
- 69% dintre atacurile hacktiviste vizează în mod direct băncile

Furt de credențiale

- Notificări false „de tip bancă” privind „activitate suspectă
- Redirecționări prin coduri QR către site-uri malițioase de colectare a credențialelo
- **Creștere anuală de 42%** a numărului de credențiale compromise puse la vânzare
- **Creștere de 500%** în log-urile de credențiale (provenite din infostealeri precum Redline, Vidar
- Brokerii de acces inițial (IAB) vând acces VPN/RDP către peste **1.400 de organizații europene**

Ransomware

- Modele de dublă / triplă extorcare (criptare + furt de date + DDoS)
- Timpul de deploy scăzut la o medie de **24 de ore**
- **92% dintre cazurile europene** implică atât criptarea fișierelor, cât și exfiltrarea datelor

Atacuri hibride fizic-ciber

- **115 atacuri asupra ATM-urilor în Germania** în 2025 (în scădere de la vârful de 496 în 2022.)
- Rețelele criminale olandeze își mută operațiunile către Austria ca urmare a măsurilor stricte de aplicare a legii în Germania

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Omisiuni frecvente ce favorizează atacurile cibernetice:

- **Neactualizarea sistemelor și aplicațiilor** - Vulnerabilitățile cunoscute rămân deschise.
- **Parole slabe sau reutilizate -** Ușor de ghicit sau de furat prin atacuri de tip credential stuffing.
- **Acces excesiv pentru angajați -** Permisiuni nejustificate pot duce la scurgeri de date.
- **Lipsa instruirii în securitate cibernetică -** Angajații devin ținte ușoare.
- **Absența autentificării multifactor (MFA) -** Doar parola nu mai oferă protecție suficientă.
- **Configurări greșite ale infrastructurii IT -** Setări incorecte în cloud, firewall sau rețele.
- **Lipsa unui plan de răspuns la incidente -** Reacția întârziată duce la pierderi și reputație afectată.
- **Neglijarea backup-urilor -** Fără copii de siguranță, recuperarea este dificilă sau imposibilă.
- **Utilizarea software-ului neautorizat -** Acesta poate conține malware sau vulnerabilități ascunse.
- **Lipsa monitorizării și detectării în timp real -** Atacurile pot trece neobservate și se pot extinde rapid.

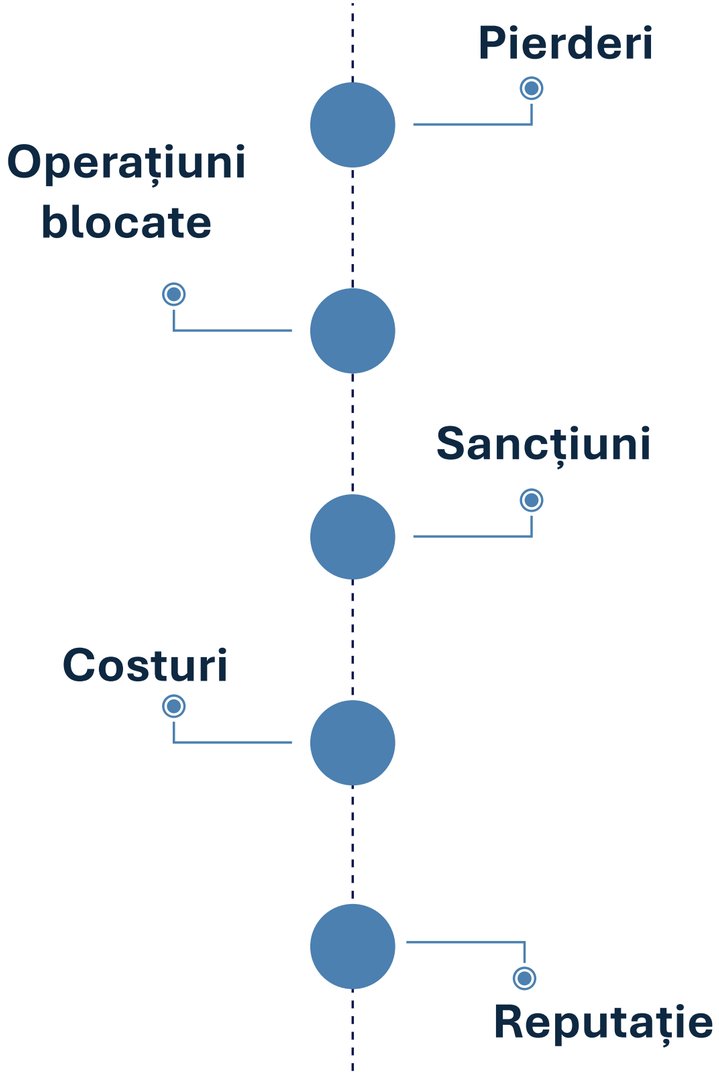
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE



Consecințe:

Pierderea datelor sensibile – informații personale, financiare sau comerciale pot fi furate sau expuse.

Oprirea operațiunilor – atacurile pot bloca sisteme critice, afectând activitatea zilnică.

Sancțiuni legale – nerespectarea normelor (ex. GDPR, NIS2) atrage penalități.

Expunerea la atacuri repetate – o breșă neadresată poate fi exploatată din nou.

Costuri financiare ridicate – recuperarea, amenzile și daunele pot ajunge la milioane.

Afectarea reputației – încrederea clienților poate fi grav deteriorată.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

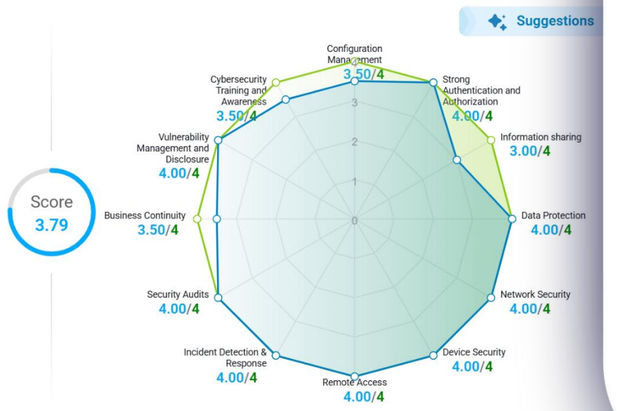
Cum ați evalua organizația dumneavoastră?

Organizație cu riscuri de securitate

O structură fragmentată, alcătuită din:

- Soluții antivirus locale
- Firewall-uri independente
- Capacități limitate de backup
- O echipă IT cu pregătire redusă în securitate

SIEMBIOT



https://nis2.siembiot.eu

Organizație modernă și protejată

O soluție SIEM centralizată care include:

- Panouri de securitate în timp real
- Integrare surse cloud, rețele și dispozitive finale
- Agregarea evenimentelor, alertelor și incidentelor
- Managementul vulnerabilităților
- O echipă IT bine pregătită, cu expertiză în securitate cibernetică

DIRECTORATUL NATIONAL
DE SECURITATE CIBERNETICA

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cum te protejează NIS2?

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cerințe NIS și soluții tehnice de securitate

Ordonanța de urgență 155/2024 este actul prin care România transpune Directiva (UE) 2022/2555 (NIS2) și stabilește noul cadru național pentru securitatea cibernetică a rețelelor și sistemelor informatice. Înlocuiește vechiul regim din Legea 362/2018 și extinde masiv aria de aplicare, tipurile de obligații și regimul sancțiunilor.
Stabilește măsurile și mecanismele necesare pentru a asigura un nivel comun ridicat de securitate cibernetică în România, pentru entitățile care furnizează servicii în sectoare esențiale și importante (conform anexelor NIS2: energie, transport, financiar, sănătate, apă, infrastructură digitală, administrație publică, spațiu, poștă, deșeuri, chimie, agro-alimentar, producție, digital providers etc.).

- Entități financiare importante
- Producția de alimente
- Sectorul energetic
- Servicii de încredere, gestionare a identităților digitale
- Transporturi
- Operatori servicii digitale, cloud, DNS
- Industria chimică
- Tratarea și distribuirea apei
- Institute de cercetare
- Managementul deșeurilor
- Sectorul medical
- Industrie spațială
- Administrație centrală și regională

Clasificare pe baza dimensiunii

Microîntreprinderi:
0- 9 angajați

Întreprinderi mici:
10 – 49 și cifră de afaceri 10mil eur

Întreprinderi mijlocii:
50 – 249 și cifră de afaceri 50mil eur

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cerințe NIS și soluții tehnice de securitate

Ordonanța de Urgență 155/2024 introduce un regim sancționator foarte sever pentru entitățile esențiale și importante, cu amenzi procentuale din cifra de afaceri globală, plus măsuri de remediere și răspundere a conducerii, în linie cu NIS2.

Sunt considerate sancțiuni: nerespectarea de către regiile autonome, societățile/companiile naționale, societățile comerciale cu capital majoritar de stat, respectiv de către autoritățile contractante, a obligațiilor NIS2

Amenzi pentru entități esențiale

• Interval general de sancțiuni: de la 10.000 lei până la 10.000.000 euro (echivalent în lei) sau până la 2% din cifra de afaceri anuală la nivel mondial, aplicându-se cuantumul mai mare.
• Aceste plafoane se aplică în special pentru încălcarea obligațiilor esențiale de management al riscului și de raportare a incidentelor, preluând logica sancțiunilor prevăzute de Directiva NIS2.

Amenzi pentru entități importante

• Interval general de sancțiuni: de la 5.000 lei până la 7.000.000 euro (echivalent în lei) sau până la 1,4% din cifra de afaceri anuală la nivel mondial, tot cu aplicarea cuantumului mai mare.
• Regimul sancționator este ușor mai redus decât pentru entitățile esențiale, dar păstrează structura procentuală din NIS2, astfel încât încălcările serioase rămân puternic descurajate

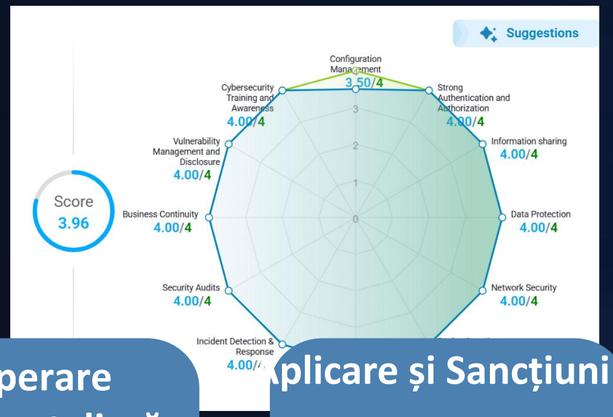
Alte sancțiuni și măsuri

• Nerespectarea obligațiilor secundare (ex. notificare, înregistrare, evaluare risc conform ordinelor DNSC) poate atrage amenzi suplimentare, de ordinul sutelor de mii de lei (până la circa 300.000 lei pentru entități importante și 500.000 lei pentru entități esențiale).

• Pe lângă amenzi, OUG 155/2024 prevede competențe extinse pentru autoritatea competentă (DNSC): ordine de remediere, termene de conformare, eventuale măsuri asupra certificărilor și creșterea răspunderii organelor de conducere pentru încălcarea obligațiilor de guvernanță și management al riscului.

expertware

Cerințele de securitate NIS impun utilizarea unor soluții tehnice avansate



Guvernanță și Responsabilitate

Existența ofițerilor de securitate

Supraveghere la nivelul consiliului de administrație

Raportarea Incidentelor

Termene de raportare: **24h**

Rapoarte detaliate de urmărire: **72h**

Managementul Riscurilor

Evaluare cuprinzătoare a riscurilor

Securitatea lanțului de aprovizionare

Conștientizare și Instruire

Instruire periodică privind securitatea cibernetică

Training pentru răspuns la incidente

Cooperare Transfrontalieră

Colaborare între statele membre

Participare la exerciții de securitate cibernetică

plicare și Sancțiuni

Amenzi semnificative

Răspundere juridică

SIEMBIOT® – Soluție pentru conformitatea cu cerințele de securitate NIS2

SIEMBIOT®

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

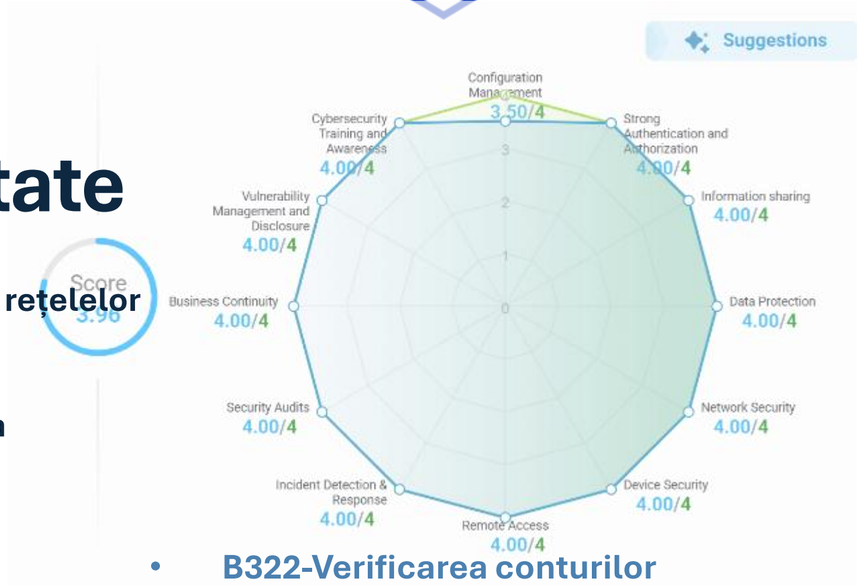
SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cerințe NIS și soluții tehnice de securitate



Directiva NIS impune organizațiilor să adopte măsuri tehnice specifice pentru protejarea rețelelor și sistemelor informatice.

Aceste cerințe includ implementarea de soluții precum monitorizare continuă, detecție a amenințărilor și răspuns automatizat la incidente:

- A191-Inventarierea și gestionarea activelor
- B111-Arhitectura NIS
- B121-Suporți de memorie externă
- B131-Segregarea și segmentarea rețelelor
- B141-Filtrarea fluxurilor
- B151-Asigurarea protecției criptografice
- B152-Managementul cheilor de criptare
- B161-Protecție malware
- B211-Conturi de administrare
- B221-Utilizarea sistemelor
- B231-Lucrul la distanță
- B311-Identificarea utilizatorilor
- B312-Autentificarea utilizatorilor
- B321-Acordarea drepturilor de acces
- B322-Verificarea conturilor privilegiate
- B411-Menținere securitate
- B412-Actualizare resurse
- B421-Sisteme de control industriale
- B422-Limitarea accesului

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

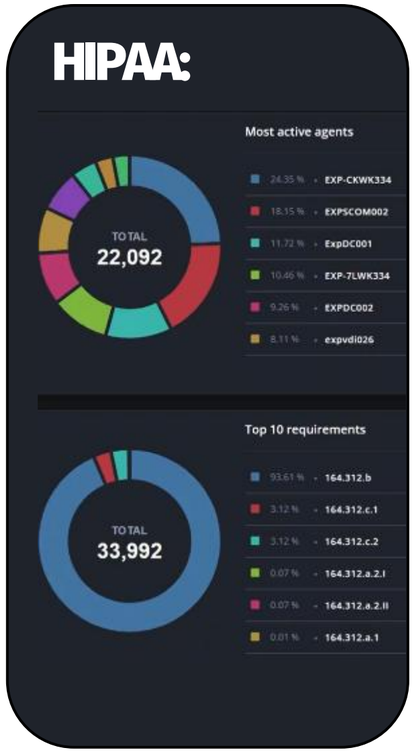
Co-funded by the European Union

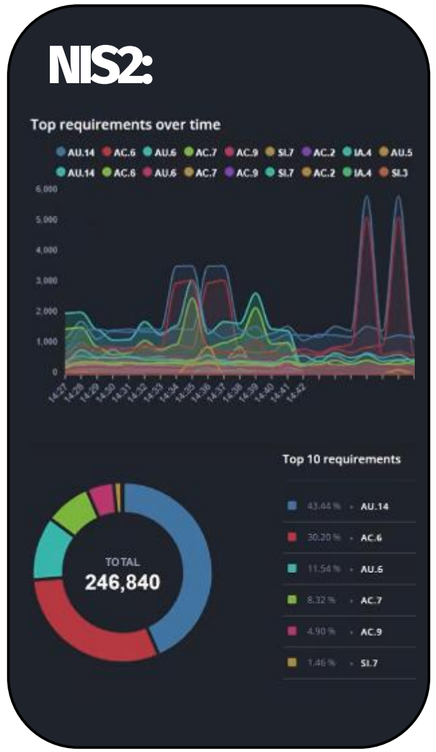
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

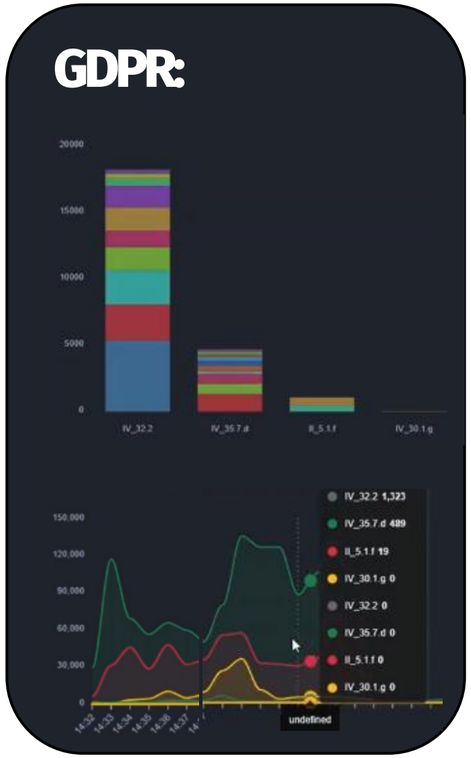
Drumul către conformitate (NIS2, HIPAA, GDPR)

Rămâi cu un pas înaintea amenințărilor prin:

- **Autoevaluare și audituri interne**
- **Monitorizare proactivă și gestionarea alertelor**
- **Scanare automată a vulnerabilităților**
- **Evaluări de risc conforme CIS**
- **Educare în securitate cibernetică**
- **Gestionarea identităților și a accesului**
- **Inventariere hardware și software**
- **Gestionarea rapidă a incidentelor**
- **Asistent AI pentru securitate**







DIRECTORATUL NATIONAL
DE SECURITATE CIBERNETICA

SIEMBIOT®

Powered by expertware

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

CE ESTE SIEMBIOT?

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

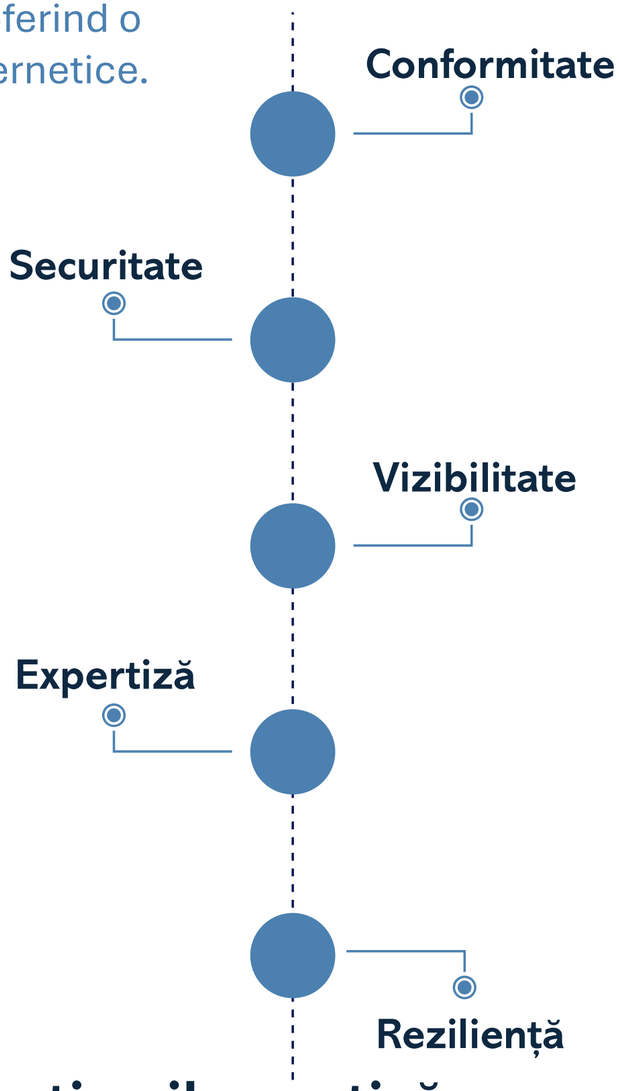
SIEMBIOT®

Powered by expertware

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Platformă **100% românească** care facilitează protecția și conformitatea cibernetică, completând și întregind soluții altfel disparate, oferind o șansă reală de minimizare a riscurilor cauzate de atacuri cibernetice.



Soluție integrată care redefinește protecția cibernetică

SIEMBIOT®

APIs | Databases | Legacy Apps | Cloud | Network Devices | Systems & Infrastructure

ASM + CTI + Dark Web ⟷ SIEM + NDR + VM + OS Compliance ⟷ SOAR Playbooks

SOC Analyst L1- L3

Threat Hunting

Malware disect / Sandboxing

Ai Agent

I'm here to help!

Security Incident Response

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funcționalități principale și indicatori

1. Managementul dispozitivelor	2. Vulnerabilități si investigare a amenințărilor	3.Informații despre noi amenințări cibernetice	4. TENANT dedicat și securizat	5. Rapoarte în timp real
Vizibilitate completă asupra tuturor dispozitivelor și a software-ului instalat pe acestea (endpoint-uri, servere, identități, rețele, chiriași cloud).	**Detectare continuă a vulnerabilităților, cu raportare detaliată.**	**Acces la peste 20 de surse care oferă informații actualizate despre amenințările de securitate.**	**Informațiile sunt stocate într-o zonă securizată cu peste 30 de conectori și peste 5000 de alerte active.**	**Interfață de administrare care permite descoperirea pericolelor si identificarea vulnerabilităților.**
10+ sectoare industriale acoperite, inclusiv administrație publică, educație, energie, finanțe, sănătate, IT, telecomunicații, cercetare și transport.	5.000.000+ vulnerabilități detectate și prioritizate 30.000+ alerte de securitate gestionate lunar. 7.000+ incidente de securitate rezolvate lunar.	79.000.000+ de înregistrări Cyber Threath Intelligence (CTI) STYX integrate și analizate.	70.000+ reguli automate de detecție SIEM pentru atacuri complexe.	100+ evaluări de conformitate NIS2 și CRA.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- User interface and reporting
- Dedicated tenant
- Cyber Threat Intelligence
- Asset Management
- Vulnerability Scanning
- Advanced Threat Hunting

- **10.000 dispozitive & utilizatori înrolați (număr în creștere)**
- **30 de organizații europene medii și mari** conectate active
- **70.000+ de reguli automate de detecție SIEM** create pentru identificarea atacurilor complexe
- **5.000.000+ de vulnerabilități detectate și prioritizate lunar**
- **3.0000+ de alerte de securitate gestionate lunar**
- **7.000+ de incidente de securitate rezolvate lunar**
- **30.000 de evenimente de securitate procesate zilnic** pentru detecție, analiză și prevenție
- **79.000.000+** de înregistrări **CTI** (Cyber Threat Intelligence) STYX analizate
- **13.000+** de articole de știri din domeniul cybersecurity moderate
- **30+ cursuri de awareness disponibile**, cu aplicații practice și scenarii reale
- **10+ sectoare acoperite**, inclusiv administrație publică, educație, energie, finanțe, sănătate, IT, telecomunicații, cercetare și transport
- **100+ de evaluări de conformitate NIS2 & CRA** realizate
- **110+ experți în securitatea cibernetică care contribuie la cercetare, monitorizare și securitate operațională**

expertware

2025
10 mil EUR

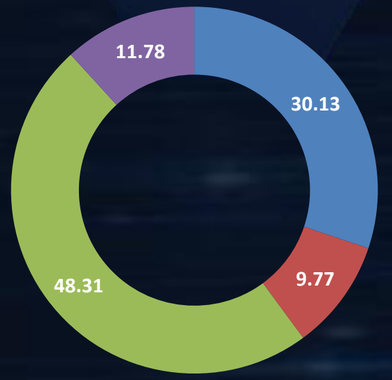
19+
Years

110+
Employees

250+
Certifications

200+
Clients

500+
Projects



- Cyber Security
- Development, BPO
- Hybrid Cloud managed services
- BI, Analytics & ML

SIEMBIOT®

DIRECTORATUL NATIONAL
DE SECURITATE CIBERNETICA

SIEMBIOT®

Powered by epertware

epertware

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

24h/7 managed security services with granular service levels

Top European Customers with **multi-billion $ yearly revenues**.
100% large customer retention in the last **6 years**.

Large European MSPs (Econocom, Getronics, Telenet) trust us **as sole partner** for **Cybersecurity , BI, Hybrid-Cloud & Bespoke Development services.**

Year on year expansion with **1-2 blue-chip customers**.
Flexible support in : **English**, French, German, Romanian

Capability to bring rapid **business value (-25% TCO, + 25% productivity)** with the right mix of IT services (BI, analytics, workspace, cybersecurity)

Beneficiary of **4 European Innovation Grants** in the field of Cybersecurity.
~7 mil EUR byget for the next 3 years.

Our customers recommend us

	Yearly turnover
BNP PARIBAS FORTIS	9.642 miliarde EUR
Audi	6.180 miliarde EUR
econocom	2.718 miliarde EUR
telenet	2.700 miliarde EUR
ENGIE	93,9 miliarde EUR
ERGO	20 miliarde EUR
Revantage / Blackstone	$326 miliarde managed

Co-funded by the European Union ECCC DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

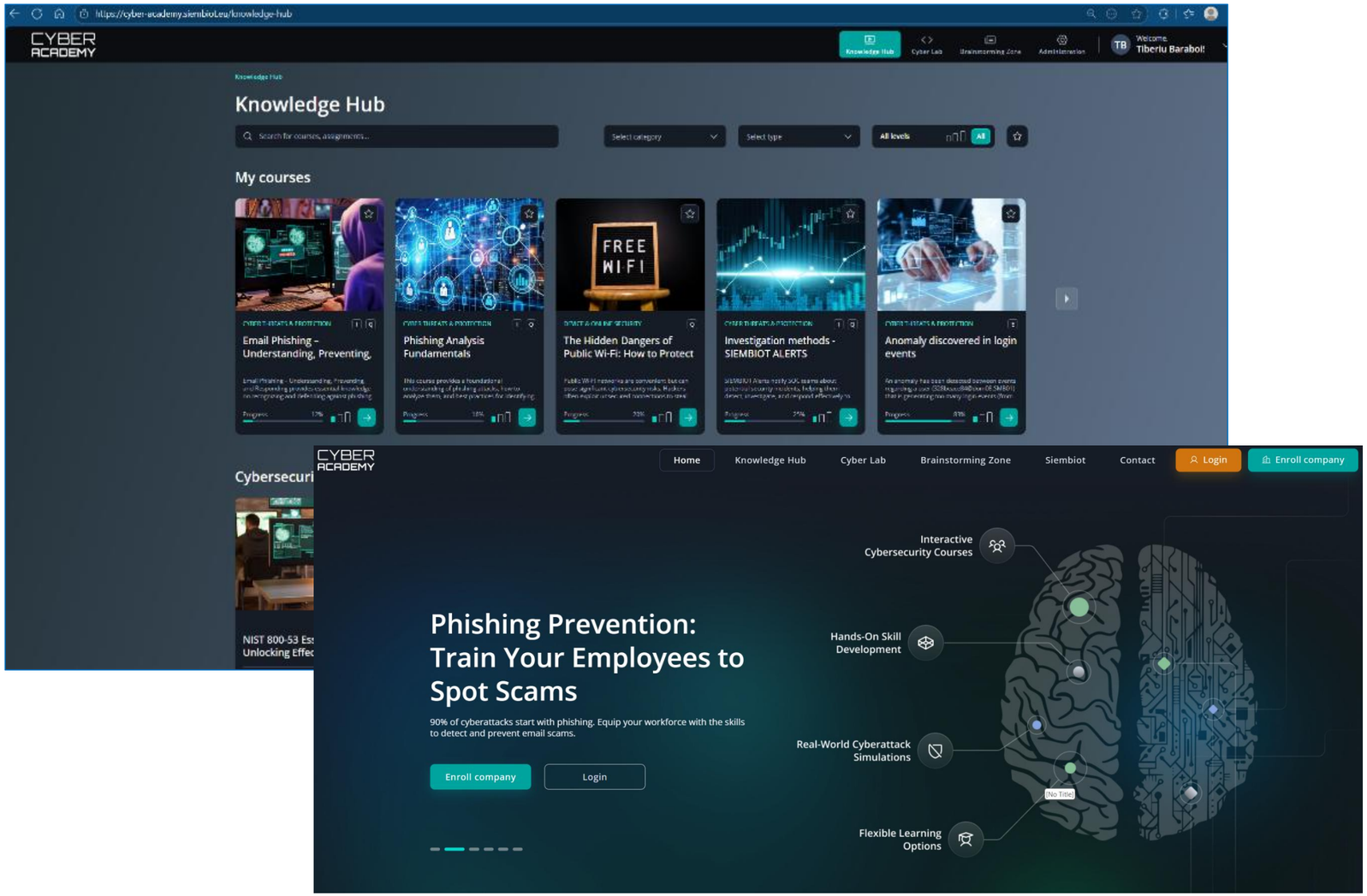
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE



Pentru că o platformă este la fel de eficientă precum echipa care o utilizează, am creat **Cyber Academy** - un spațiu dedicat dezvoltării echipei tale, unde aceasta poate beneficia de:

- Sesiuni practice de instruire în domenii precum ”phishing”, ”malware”, ”ransomware”, investigații și multe altele
- Învață standardele și cele mai bune practici în securitate cibernetică
- Exersează în medii interactive, concepute pentru a simula scenarii reale cu care se confruntă analiștii de securitate

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

SIEMBIOT®

Powered by expertware

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Informații follow-up:

Nu ezitați să ne contactați dacă aveți nevoie de detalii suplimentare.

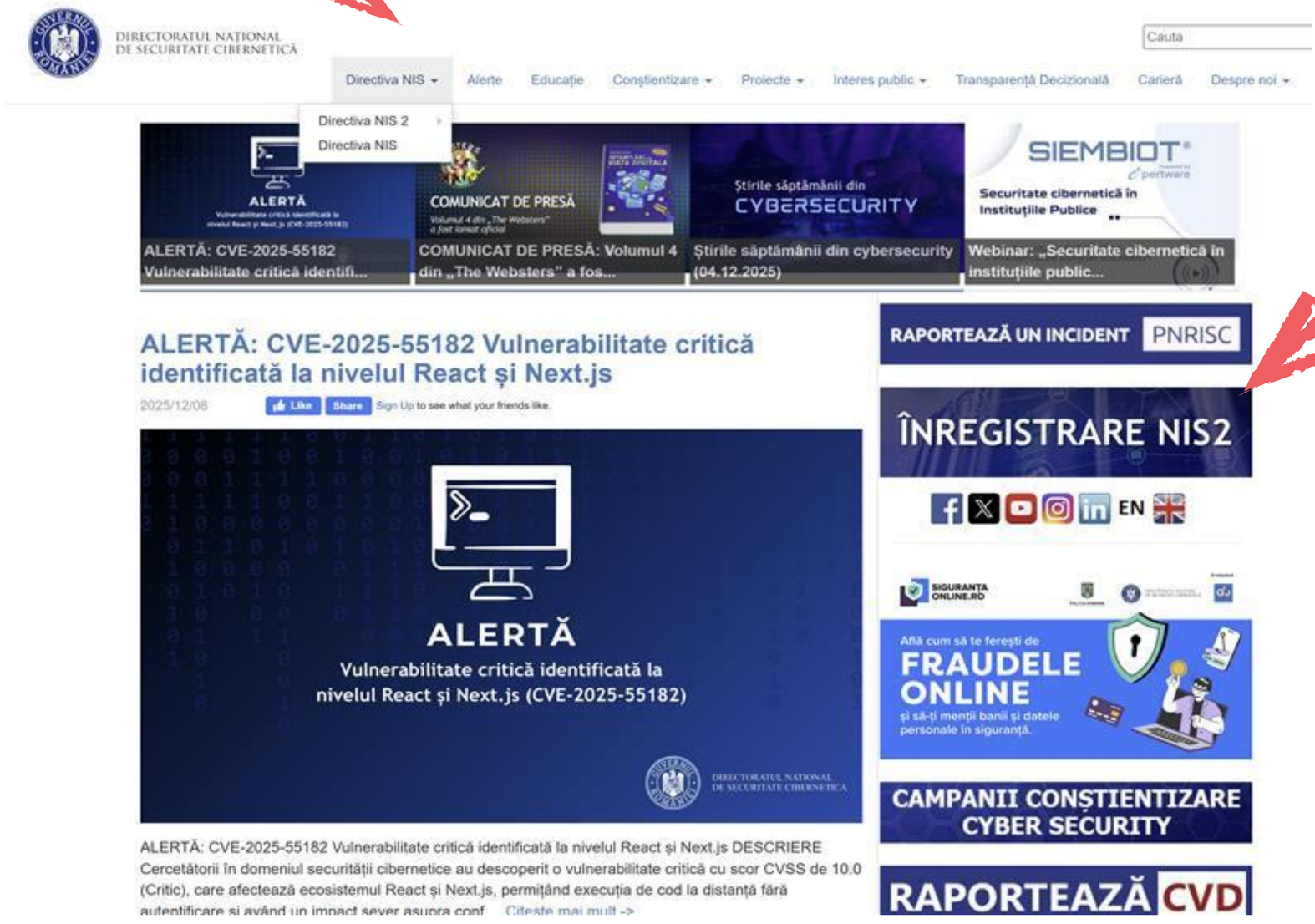
- O prezentare video și un ghid de utilizare pentru platforma SIEMBIOT.
- O demonstrație live completă a funcționalităților platformei.
- O discuție tehnică privind caracteristicile SIEMBIOT.
- Orice alte informații sau clarificări de care aveți nevoie.

Accesati formularul de pe site pentru cerere demo:
https://siembiot.eu/#free-trial

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

DIRECTORATUL NATIONAL
DE SECURITATE CIBERNETICA

Legislație NIS2



Înregistrare NIS2

www.dnsc.ro