DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Securitate cibernetică în domeniul sănătății

Obligații NIS2 și oportunități prin platforma SIEMBIOT

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CUPRINS

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

01

Contextul Actual al Amenințărilor Cibernetice

Tendințe și cifre relevante în sănătate

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ
expertware
SIEMBIOT®
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Importanța securității cibernetice în domeniul sănătății

Digitalizarea serviciilor medicale

- sistemele HIS, EHR și EMR sunt utilizate zilnic în spitale publice și clinici private
- laboratoarele, imagistica și raportările către CNAS funcționează în infrastructuri IT conectate permanent

Cum sunt vizate unitățile medicale

- ransomware care criptează serverele și blochează accesul la datele pacienților
- phishing direcționat către personal administrativ și financiar
- acces obținut prin furnizori IT sau servicii de mentenanță externă

Impactul direct asupra activității medicale

- imposibilitatea accesării fișelor medicale și a rezultatelor de laborator
- revenirea temporară la proceduri pe hârtie
- întârzieri în internări, externări și raportări către autorități

Contextul Amenințărilor în Sănătate

289+

Incidente cyber în UE healthcare (2024)

71%

Atacuri ransomware care afectează îngrijirea

€300K

Cost mediu per incident major

92%

Organizații care au raportat atacuri în 2024

Sectorul sănătății a raportat cele mai multe incidente din toate sectoarele critice UE în 2023–2024.
Costul mediu al unei brese de date în healthcare a ajuns la $9.77M (IBM 2024). Grupuri pro-Rusia precum Killnet și Anonymous Sudan au lansat atacuri DDoS coordonate asupra spitalelor din UE.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

02

Sisteme Critice în Spitale și Clinici

HIS / EHR, PACS / Imagistică, IoMT

Ce sisteme sunt considerate critice?

HIS / EHR

Hospital Information System
Electronic Health Records

- Gestionează datele pacienților, internări, rețete, facturare
- Centralizează întreaga activitate clinică
- Dacă sunt afectate, spitalul trece pe hârtie și pix
- Exemplu RO: Platforma Hipocrate

PACS / Imagistică

Picture Archiving and
Communication System

- Stochează și distribuie imagini medicale (CT, RMN, Rx)
- Protocol DICOM – adesea necriptat
- Downtime = amânare diagnostic și tratamente
- Nu poate fi oprit pur și simplu pentru un patch

IoMT

Internet of Medical Things
Echipamente Conectate

- Pompe de infuzie, monitoare pacient, ventilatoare
- Rulează OS embedded – fără update-uri regulate
- Comunică pe rețeaua spitalului, adesea nesegmentat
- 5G extinde suprafața de atac

Ce nu poate fi oprit sau patch-uit ușor

Sistemele critice din spitale au constrângeri unice față de mediul enterprise clasic

Dispozitive medicale cu firmware legacy

Echipamente cu cicluri de viață de 10–15 ani. Rulare pe Windows XP/7, fără suport vendor. Patch-urile pot invalida certificări FDA/CE.

Rețele flat / nesegmentate

VLAN-uri comune pentru administrativ, clinic și IoMT. Mișcarea laterală este trivială după compromiterea inițială.

Sisteme HIS/EHR cu uptime 24/7

Nu există fereastră de mentenanță. Orice restart afectează îngrijirea pacienților. Configurații nestandardizate între spitale.

Protocoale vechi și necriptate

DICOM, HL7v2, Telnet – nu au fost proiectate cu securitate. Multe nu suportă TLS sau autentificare modernă.

Backup-uri inaccesibile sau netestate

Lipsa backup-urilor offline. Testarea restaurării nu se face periodic. Un spital din România avea ultimul backup de acum 12 zile.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

03

Tipare Reale de Atac în Domeniul Medical

Cazuri concrete din România și Uniunea Europeană

Atacul Ransomware asupra Spitalelor din România

FEBRUARIE 2024 | Backmydata / Phobos Ransomware

VECTOR DE ATAC

Platforma HIS Hipocrate – provider unic de servicii pentru zeci de spitale

RANSOMWARE

Backmydata (familia Phobos) – folosit via acces RDP cu credentiale slabe

RĂSCUMPĂRARE

3.5 BTC (~€157.000) – nu a fost plătită

CRONOLOGIE

10 Feb – Spitalul Pediatric Pitești (primul); 11–12 Feb – atacuri în masă

IMPACT

- 26 spitale cu date criptate
- 100+ unități deconectate preventiv
- 400+ calculatoare și servere afectate
- Doctori trecuți pe hârtie și pix
- Analize de sânge tipărite manual
- Facturare CNAS blocată
- Bitdefender implicat în recuperare
- DNSC a coordonat răspunsul național

Lecție: Un singur furnizor HIS compromis a declanșat un efect de domino în tot sistemul de sănătate din România. Lipsa segmentării, dependența de un singur vendor și expunerea RDP au fost factorii determinanți.

Atacuri High-Profile în Uniunea Europeană

Synnovis / NHS UK – Iunie 2024

Qilin Ransomware | Răscumpărare: $50M

- A atacat laboratorul de patologie Synnovis din Londra
- 7 spitale NHS afectate (King's College, Guy's & St Thomas')
- 1.134 operații anulate + 2.194 consultații în primele 13 zile
- Teste de sânge la 10% din capacitatea normală
- 400 GB date pacienți exfiltrate și publicate pe darknet
- Un deces confirmat legat de întârzierea analizelor
- Recuperare completă: 17+ luni

Alte Cazuri Notabile

Universitätsklinikum Düsseldorf (2020)
Primul deces atribuit unui cyberatac – redirectarea ambulanței a cauzat decesul unui pacient

Change Healthcare / UnitedHealth (Feb 2024)
100 milioane americani afectați – cea mai mare breșă din istoria healthcare-ului. Perturbarea lanțului de aprovizionare farmaceutic.

Grupuri pro-Rusia (Killnet) – 2023-2024
Atacuri DDoS coordonate asupra spitalelor din Danemarca, Germania, Olanda. Parte din războiul hibrid.

AZ Monica Hospital/Antwerp, Belgia (2026)
70+ de operații anulate, 7 pacienți transferați, imagistica și chimioterapia au fost suspendate. Acces indisponibil la dosarele electronice ale pacienților. Sistemele IT au fost restaurate după o lună.

TEHNICI EMERGENTE

- **Atacuri CAPTCHA false:** peste 1.000 în Europa (2024-2025)
- **Furt de credențiale asistat de AI:** automatizarea atacurilor
- **Ransomware pe ESXi:** atacuri care vizează infrastructuri virtualizate (ex.: gruparea Scattered Spider)
- **Tactici cross-domain:** grupuri eCrime din Vest care demonstrează un nivel de sofisticare comparabil cu APT-urile.

AMENINȚĂRI ÎN SECTORUL MEDICAL

- **Costuri ridicate ale breșelor** în sectorul medical
- **Creșterea incidentelor cibernetice** raportate de spitale
- **Expunerea datelor pacienților** și obligații de notificare
- **Ransomware asupra sistemelor clinice**, cu blocaje operaționale

În 2024, Comisia Europeană a numărat 289+ incidente de securitate în sectorul sănătății – mai multe decât în orice alt sector critic.

04

Gap-uri recurente observate

Vulnerabilități sistematice în mediul medical

Gap-uri Recurente în Securitatea Cibernetică Medicală

Lipsa segmentării rețelei

Rețele flat: IT, medical și IoMT pe același VLAN. Mișcarea laterală este trivială.

Patch management inexistent

Dispozitive legacy pe Windows XP/7. Patch-urile anulează certificări sau nu există.

Acces RDP expus

Credențiale slabe pe RDP public. Vector #1 pentru Phobos/Backmydata în RO.

Backup-uri netstestate

Fără backup offline. Fără testare restaurare. Unele spitale: backup vechi de 12+ zile.

Dependență de vendor unic

Un singur provider HIS (ex: Hipocrate) pentru zeci de spitale – single point of failure.

Lipsa SOC / SIEM

Fără monitorizare continuă 24/7. Atacurile sunt detectate doar la criptare, nu la intruziune.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

05

Relația cu NIS2 Perspectivă Tehnică

Ce cere directiva și ce înseamnă practic pentru spitale

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

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 de administrare
- 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

NIS2 – Obligații Tehnice pentru Healthcare

Spitalele sunt entități esențiale (Anexa I) – cel mai înalt nivel de cerințe și sancțiuni

CERINȚE TEHNICE CHEIE

- Analiză de risc și politici de securitate IT/OT/IoMT
- Segmentare rețea și izolarea sistemelor critice
- MFA obligatoriu + criptare end-to-end
- Incident Response Plan testat periodic
- Backup-uri offline, testate, cu restaurare verificată
- Evaluarea securității furnizorilor (supply chain)
- SIEM/SOC pentru detecție și răspuns 24/7
- Training cybersecurity pentru personal

RAPORTARE INCIDENTE

24h	Early warning către autoritatea competentă
72h	Notificare inițială cu detalii tehnice
1 lună	Raport final complet

SANCȚIUNI

Până la €10M

sau 2% din cifra de afaceri globală

Răspundere personală a managementului

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

06

SIEMBIOT®

De la evaluare la protecție operațională

Plan 90 Zile - Implementare SIEMBIOT

ZILELE 1-30

EVALUARE & ONBOARDING

- Audit NIS2 readiness inițial
- Inventar complet: IT, OT, IoMT
- Conectare surse de log la SIEMBIOT SIEM
- Mapare asset-uri pe MITRE ATT&CK
- Scan vulnerabilități pe întreaga rețea
- Activare CTI feeds (AlienVault, MISP)
- Definire primele reguli de detecție

ZILELE 31-60

HARDENING & DETECȚIE

- Segmentare rețea: IT vs. clinic vs. IoMT
- Implementare MFA pe sisteme critice
- Tuning reguli SIEM – reducere false pozitive
- Integrare Vulnerability Management continuu
- Configurare backup offline + test restaurare
- Creare playbook-uri de incident response
- Training echipe IT și personal medical

ZILELE 61-90

OPERAȚIONALIZARE SOC

- Monitorizare 24/7 prin SOCaaS SIEMBIOT
- 47 threat-hunting queries active
- Testare plan de răspuns la incidente
- Rapoarte compliance NIS2 automatizate
- Simulare atac (table-top exercise)
- Review cu management – dashboard KPI
- Tranziție la operațiuni continue

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SIEMBIOT – Platformă Unificată de Cybersecurity

Dezvoltat de Expertware în colaborare cu DNSC și finanțat de Uniunea Europeană

SIEM Avansat

Vizibilitate real-time, alertare inteligentă și forensics în medii cloud, on-prem și hibride.

Vulnerability Management

Identificare, prioritizare și remediere continuă a riscurilor pe toate asset-urile.

Cyber Threat Intelligence

CTI live integrat în workflow-uri. Surse: AlienVault, MITRE, AnyRun, MISP + 10 feed-uri.

AI-Powered Detection

Învățare din mediul tău. Alerte explicate în limbaj clar. Sugestii automate next-step.

Compliance NIS2 Built-in

Rapoarte pre-construite, logging centralizat, RBAC, suport GDPR și ISO 27001.

SOCaaS pentru Healthcare

Monitorizare 24/7, răspuns la incidente, training pe date anonimizate. Fără echipă internă.

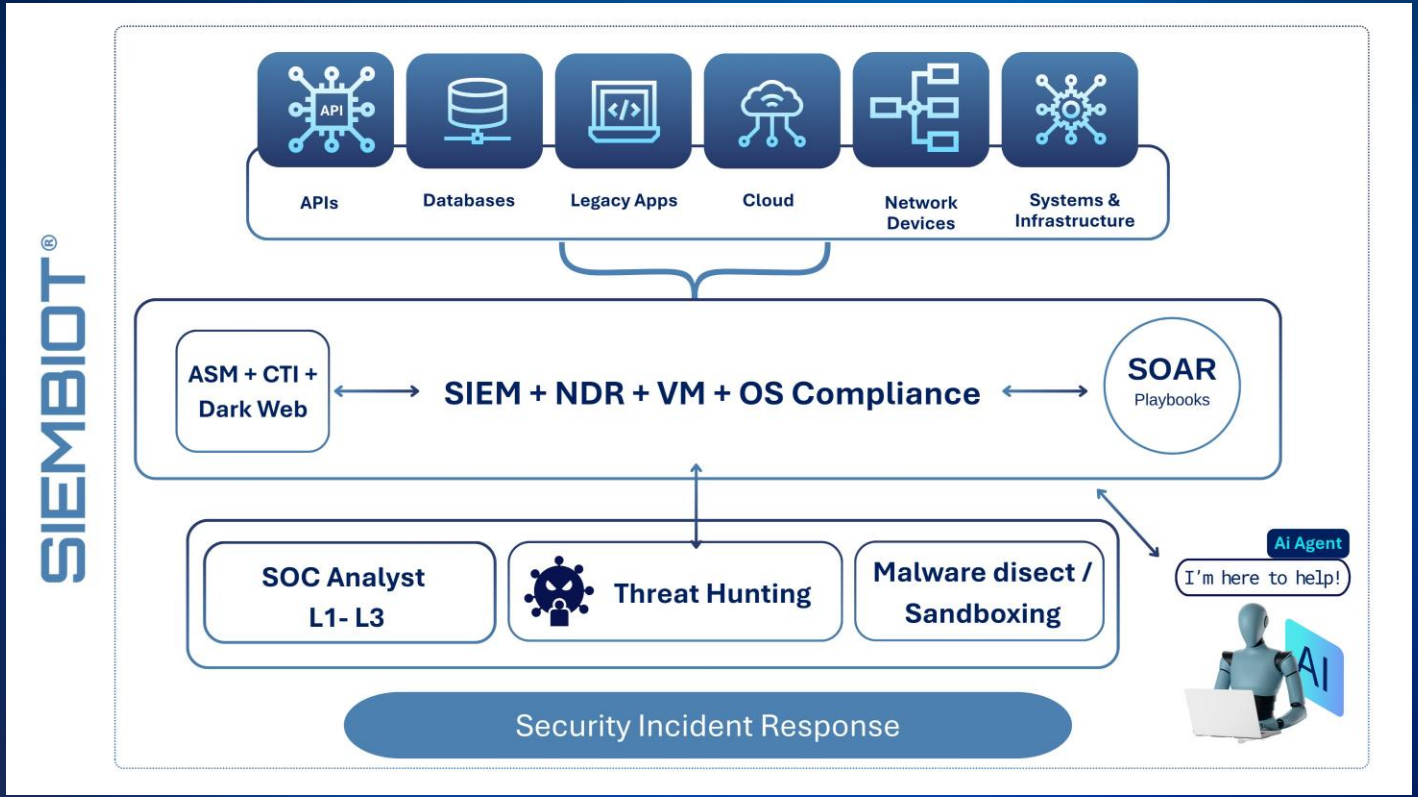
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE



DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

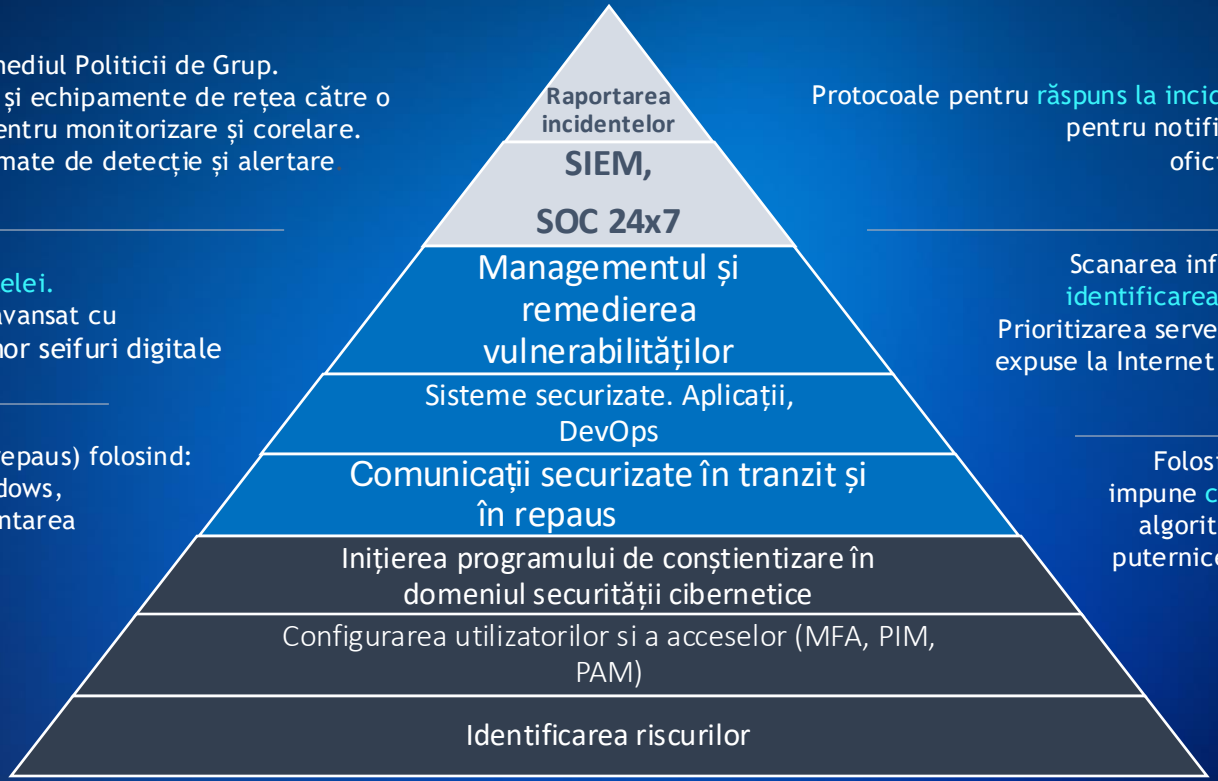
Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Configurați auditul prin intermediul Politicii de Grup.
Trimitere logurilor de la stații și echipamente de rețea către o platformă centralizată SIEM pentru monitorizare și corelare.
Implementarea de reguli automate de detecție și alertare.

Segmentarea și protejarea rețelei.
Implementarea unui firewall avansat cu funcționalități de IDS/IPS a unor seifuri digitale securizate

Criptarea datelor stocate (în repaus) folosind:
BitLocker pentru sisteme Windows,
LUKS pentru Linux și implementarea de backup-uri criptate..



Protocoale pentru răspuns la incidente de securitate pentru notificare și comunicare oficială a incidentelor.

Scanarea infrastructurii pentru identificarea vulnerabilităților.
Prioritizarea serverelor și aplicațiilor expuse la Internet pentru remediere.

Folosirea GPOs pentru a impune criptarea bazată pe algoritmi și suite de cifru puternice la nivelul întregii infrastructurii.

https://www.enisa.europa.eu/publications/enisa-nis360-2024

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DEMO

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funcționalități principale și indicatori

1. Managementul dispozitivelor

Vizibilitate completă asupra tuturor dispozitivelor și a software-ului instalat pe acestea (endpoint-uri, servere, identități, rețele, chiriași cloud).

10+ sectoare industriale acoperite, inclusiv administrație publică, educație, energie, finanțe, sănătate, IT, telecomunicații, cercetare și transport.

2. Vulnerabilități si investigare a amenințărilor

Detectare continuă a vulnerabilităților, cu raportare detaliată.

5.000.000+ vulnerabilități detectate și prioritizate lunar .
30.000+ alerte de securitate gestionate lunar.
7.000+ incidente de securitate rezolvate lunar.

3. Informații despre noi amenințări cibernetice

Acces la peste 20 de surse care oferă informații actualizate despre amenințările de securitate.

79.000.000+ de înregistrări Cyber Threath Intelligence (CTI) STYX integrate și analizate.

4. TENANT dedicat și securizat

Informațiile sunt stocate într-o zonă securizată cu peste 30 de conectori și peste 5000 de alerte active.

70.000+ reguli automate de detecție SIEM pentru atacuri complexe.

5. Raportare în timp real

Interfață de administrare care permite descoperirea pericolelor si identificarea vulnerabilităților.

100+ evaluări de conformitate NIS2 și CRA

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ
expertware
SIEMBIOT®
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

De ce este SIEMBIOT cea mai potrivită alegere:

- Vizibilitate completă (360°) asupra organizației
- Instalarea de agenți software pe echipamentele
- Pachet complet de aplicații de top pentru monitorizare
- Interfață modernă cu rapoarte
- Inventar în timp real la nivelul întregii organizații
- Rapoarte în timp real privind alertele de securitate
- Platformă dedicată pentru gestionarea incidentelor de securitate (Incident Response)
- Rapoarte actualizate privind vulnerabilitățile (Vulnerability Management)
- Agent cibernetic bazat pe inteligență artificială

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Descoperă gratuit platforma

Cum analizăm costul securității cibernetice?

Servicii suplimentare

Ai acces gratuit timp de 3 luni, fără costuri și fără obligații.

Explorează toate funcționalitățile, testează interfața intuitivă și vezi cum poate revoluționa modul în care gestionezi securitatea cibernetică.

Recomandăm o soluție NAC integrată SIEMBIOT, pentru o monitorizare mai eficientă a rețelei.

Accesezi servicii suplimentare specializate, precum: Centrul de Operațiuni de Securitate 24x7 (SOC), Furnizor de Servicii Gestionate (MSP), Operațiuni de Rețea (NOC) și Accesului la Rețea (NAC).

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Sesiune Q&A

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

expertware

SIEMBIOT®

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

expertware

SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Sunteți pregătiți pentru pericolele cibernetice?

siembiot.eu