Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

SIEMBIOT®

CYBER ACADEMY

Platformă educațională pentru dezvoltarea competențelor în securitate cibernetică

Coordonator

Partener

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Powered by Expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Contextul actual al securității cibernetice

Digitalizarea accelerată a mediului academic

- utilizarea extinsă a platformelor online, cloud și a accesului remote
- creșterea suprafeței de atac odată cu digitalizarea proceselor educaționale

Creșterea atacurilor asupra instituțiilor educaționale

- phishing și compromiterea conturilor instituționale
- acces neautorizat la date academice și administrative

Nevoia de competențe practice în cybersecurity

- diferență între pregătirea teoretică și cerințele reale ale industriei
- cerere crescută pentru specialiști cu experiență practică

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Provocarea actuală în educația cybersecurity

- **Educația în securitate cibernetică se confruntă cu o provocare majoră:** diferența dintre cunoștințele teoretice și competențele necesare în mediile operaționale reale.
- **Instituțiile academice au nevoie de metode de învățare** care să apropie studenții de scenarii reale și procese utilizate în industrie.

Accent pe teorie

Experiență practică limitată

Diferență între cerințele industriei

Și pregătirea academică

Lipsa expunerii

La scenarii reale de securitate cibernetică

- Cyber Academy răspunde acestei provocări printr-un model educațional care combină cunoștințele teoretice cu experiența practică și colaborarea aplicată, contribuind la creșterea nivelului de maturitate în securitate cibernetică, în linie cu direcțiile NIS2.

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Cum răspunde Cyber Academy provocărilor

Aliniere la cerințele NIS2

Platforma ajută organizațiile să își pregătească personalul pentru cerințele NIS2 prin formarea unor practici corecte de securitate.

Platformă educațională pentru organizații/universități

Cyber Academy oferă cursuri și exemple practice care explică riscurile de securitate și modul în care acestea sunt gestionate în organizații.

Învățare progresivă

Participanții pornesc de la concepte de bază și ajung treptat la exerciții și scenarii practice.

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

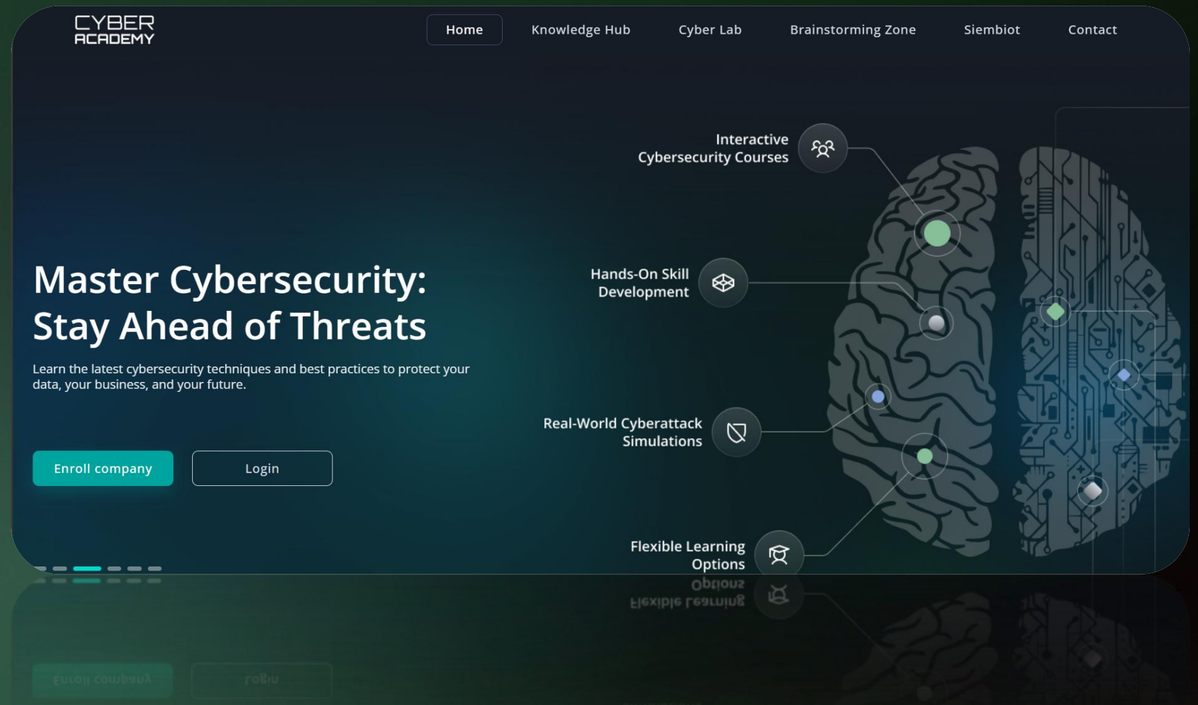
DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Cum poate fi accesată Cyber Academy

Acces simplu și flexibil pentru organizații

Cyber Academy poate fi accesată ușor de organizații printr-un **cont organizațional gratuit,** care permite adăugarea treptată a participanților în funcție de roluri și nevoi.

Accesul este public, iar implementarea poate începe gradual, printr-un program pilot adaptat structurii fiecărei organizații.



https://cyber-academy.siembiot.eu/

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

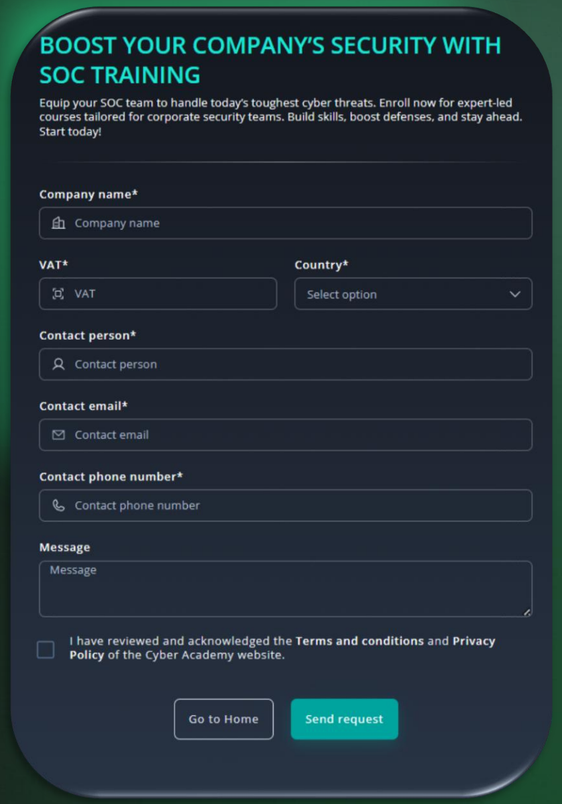
Accesul în Cyber Academy

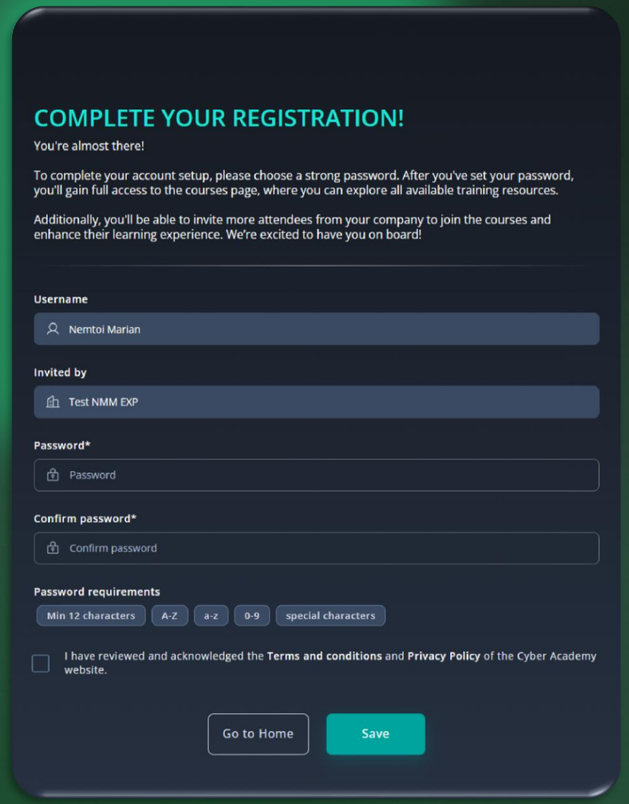
Înrolare în platformă

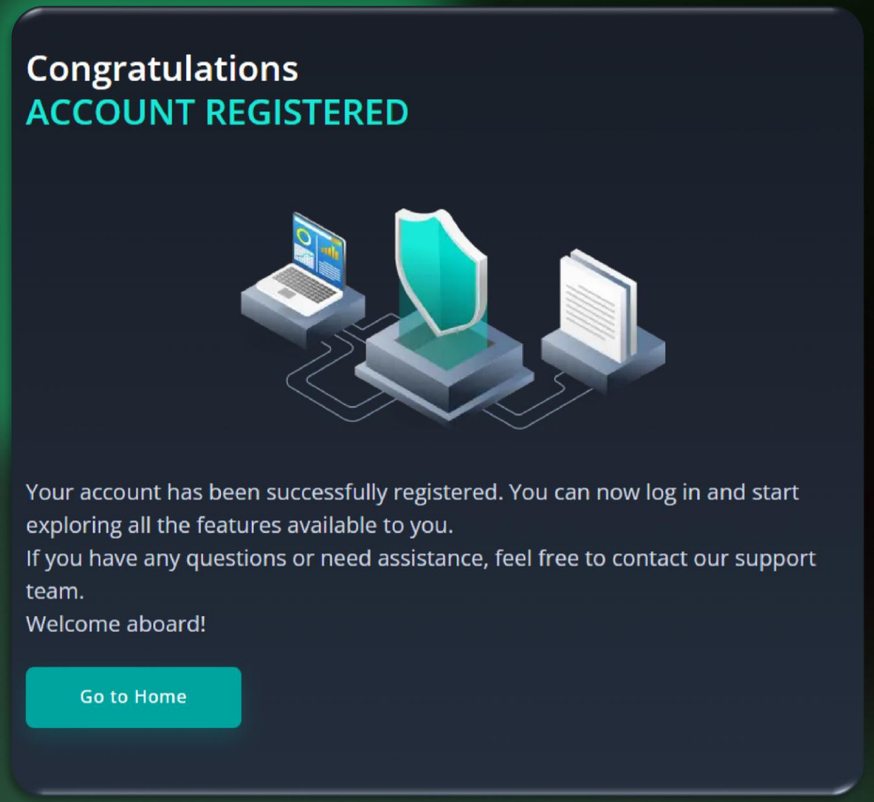
- Utilizatorul completează formularul de înscriere, iar după trimitere primește un mesaj și un email care confirmă că solicitarea este în curs de verificare.

Crearea contului

- După aprobarea solicitării, utilizatorul accesează linkul primit pe email, își setează parola și finalizează crearea contului pentru a putea accesa platforma.







Co-funded by the European Union

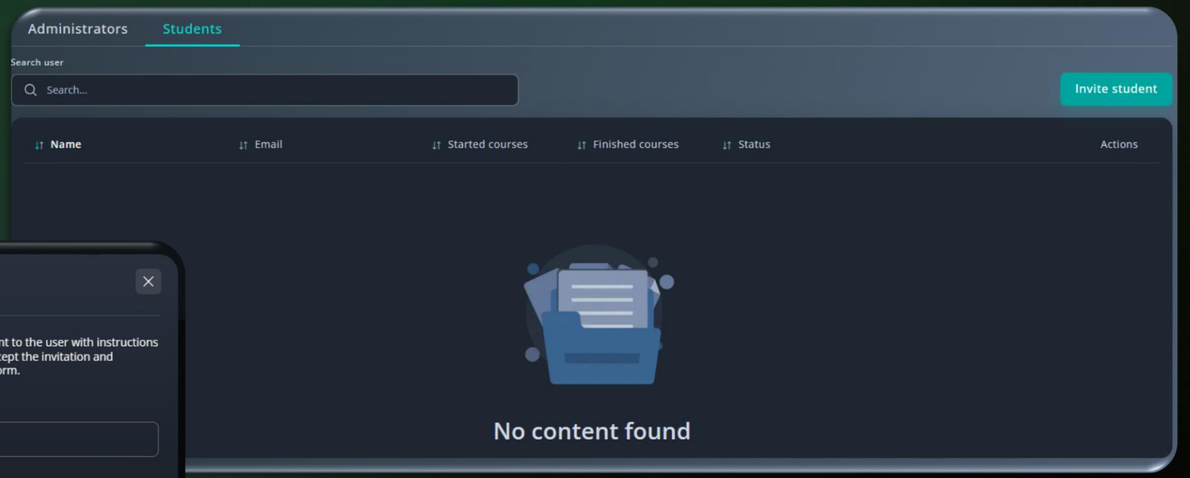
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

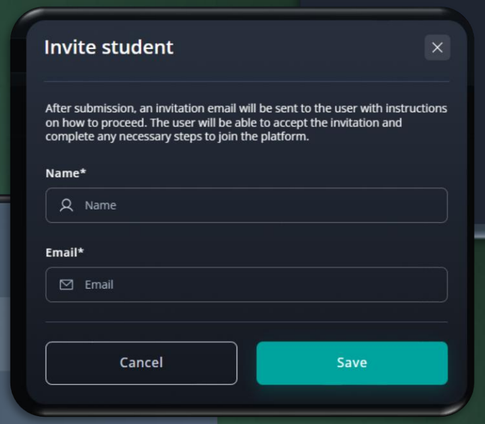
expertware

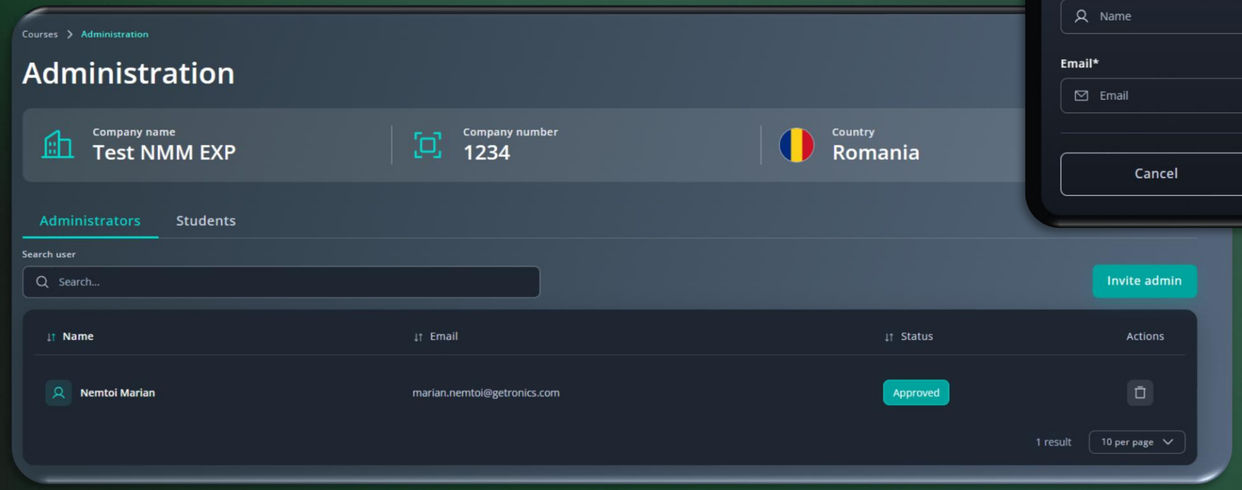
DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Administrarea organizației în Cyber Academy

- ✓ După autentificare, administratorul are acces la zona de administrare, unde poate invita administratori sau studenți și le poate oferi acces la Knowledge Hub, Cyber Lab și Brainstorming Zone.
- ✓ Doar administratorii pot adăuga utilizatori noi.







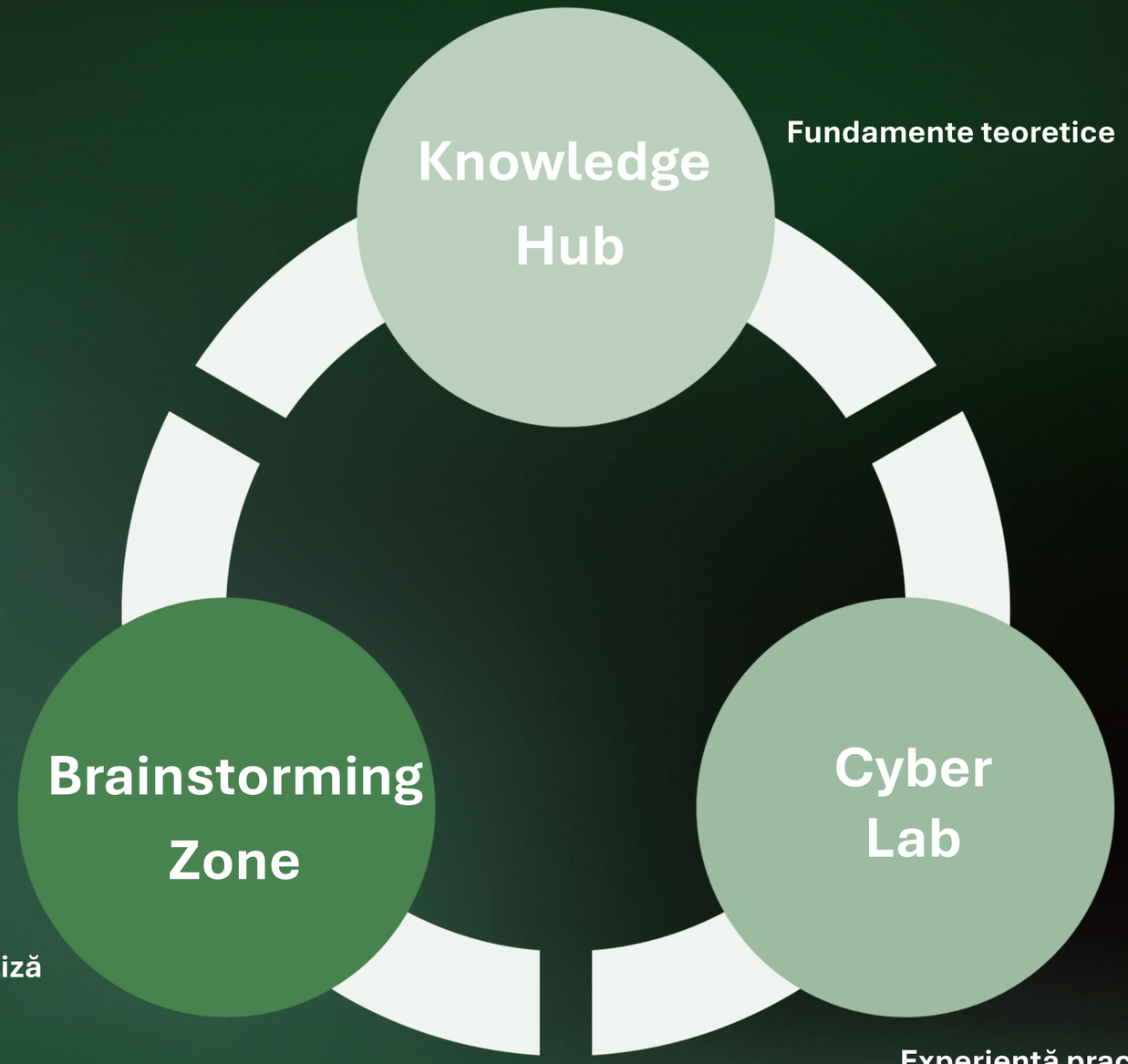
Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Structură Cyber Academy



Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Knowledge Hub = cursuri gratuite de awareness în securitate cibernetică

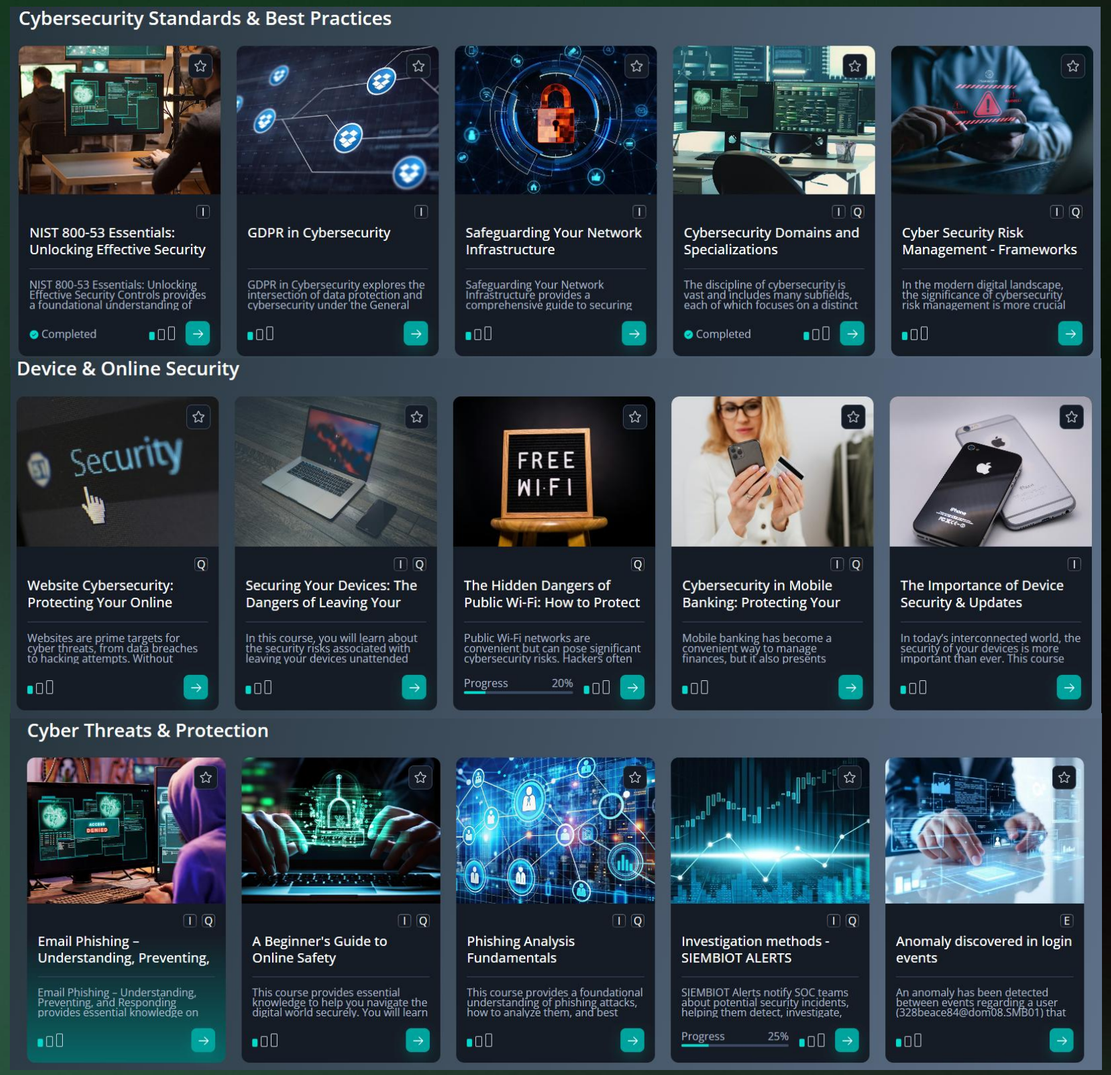
Peste 30 de cursuri, organizate pe trei direcții principale:

- ✓ **Standardele și bunele practici** în securitate cibernetică
- ✓ **Securitatea dispozitivelor** și a activităților online
- ✓ **Amenințări cibernetice** și metode de protecție

*Poți începe mai multe cursuri simultan.

**Ai posibilitatea de a întrerupe un curs în orice moment și de a-l relua ulterior, exact de unde ai rămas.

Cyber-academy.siembiot.eu/knowledge-hub



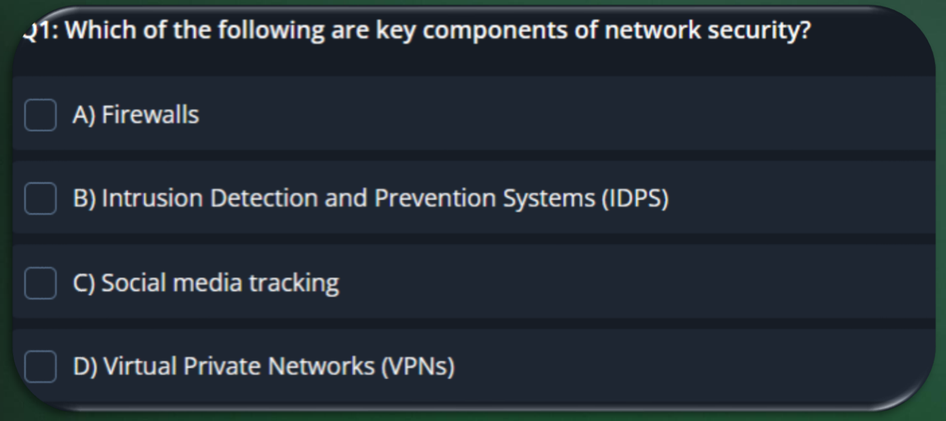
Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

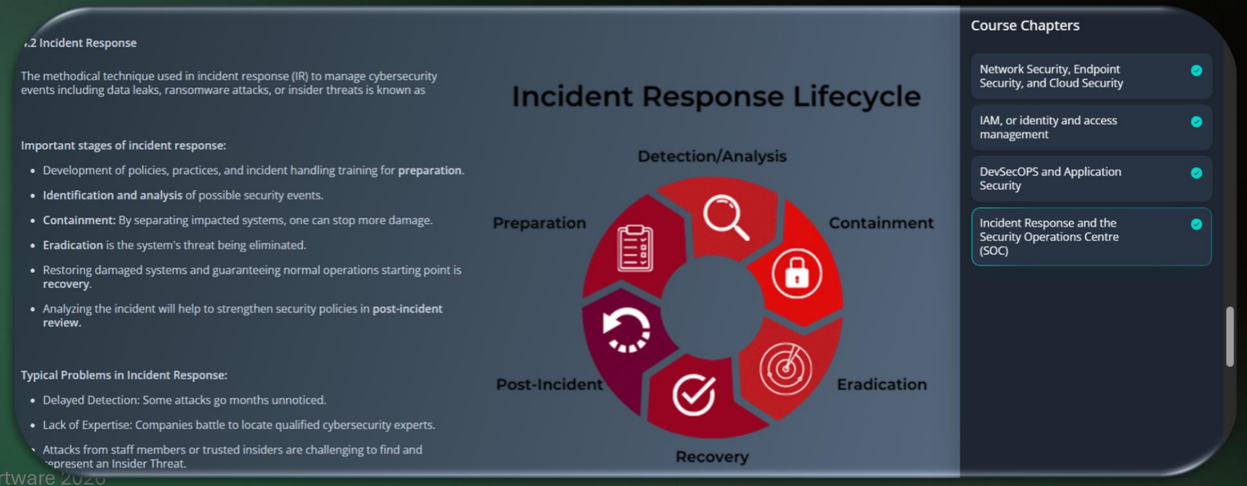
expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Structura unui curs în Cyber Academy



- ✓ Fiecare curs include o prezentare generală și un indicator al nivelului de dificultate: **Beginner/Intermediate/Advanced**
- ✓ Cursurile sunt structurate în capitole relevante, iar fiecare capitol conține toate informațiile esențiale legate de subiect.
- ✓ Zona de quiz este disponibilă pentru verificarea cunoștințelor dobândite pe parcursul cursului.



Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Cursuri de Cybersecurity Standards & Best Practices

Nivel: Beginner, Limba Engleză, Limba Română

- NIST 800-53 Essentials: Unlocking Effective Security
- GDPR in Cybersecurity
- Safeguarding Your Network Infrastructure
- Cybersecurity Domains and Specializations
- Cyber Security Risk Management - Frameworks
- Phishing Analysis Advanced Tactics
- Cybersecurity Careers: Your Path to a Future-Proof
- How to use Cyber Lab
- DQL Query Practice – Application Monitoring
- DQL Query Practice – Windows Logon Types
- DQL Query Practice – Windows Group
- Social Engineering
- Methods for detecting open ports
- OSINT Foundations in Cybersecurity Operation
- **ANEXA 2 – Deepfake (Limba Română)**
- **Protejarea si recuperarea conturilor de social media (Limba Română)**
- **Elemente esențiale de securitate cibernetică (Limba Română)**

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

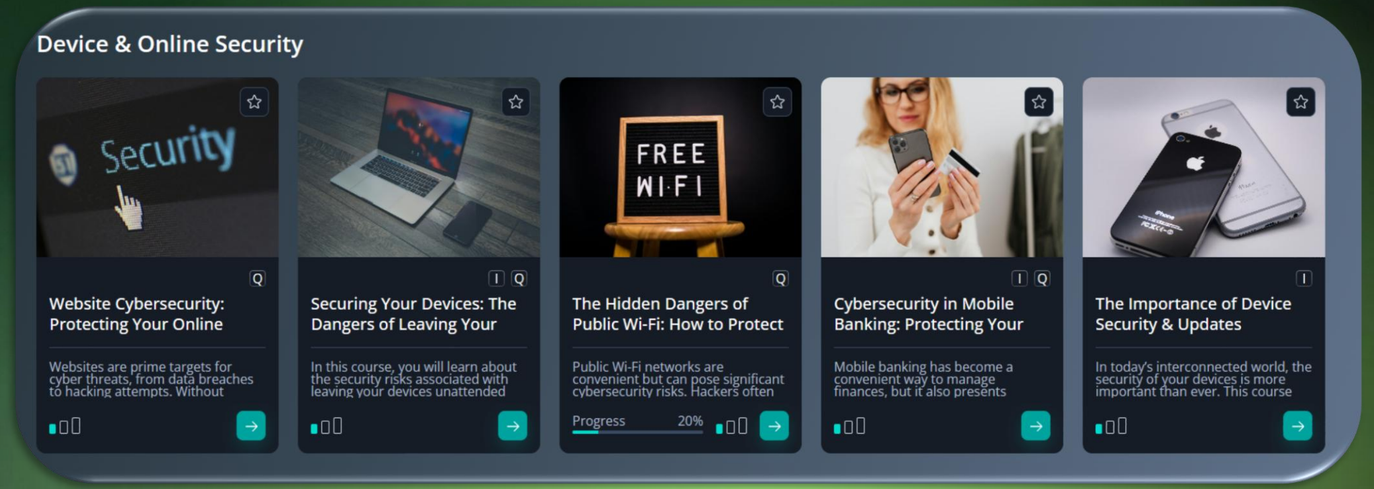
expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Cursuri de Device & Online Security

Nivel: Beginner, Limba Engleză

- Website Cybersecurity: Protecting Your Online
- Securing Your Devices: The Dangers of Leaving Your
- The Hidden Dangers of Public Wi-Fi: How to Protect
- Cybersecurity in Mobile Banking: Protecting Your
- The Importance of Device Security & Updates
- Install application attempt generated by a privileged or non-privileged account
- Web application penetration testing



Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Cursuri de Cyber Threats & Protection

Nivel: Beginner, Limba Engleză

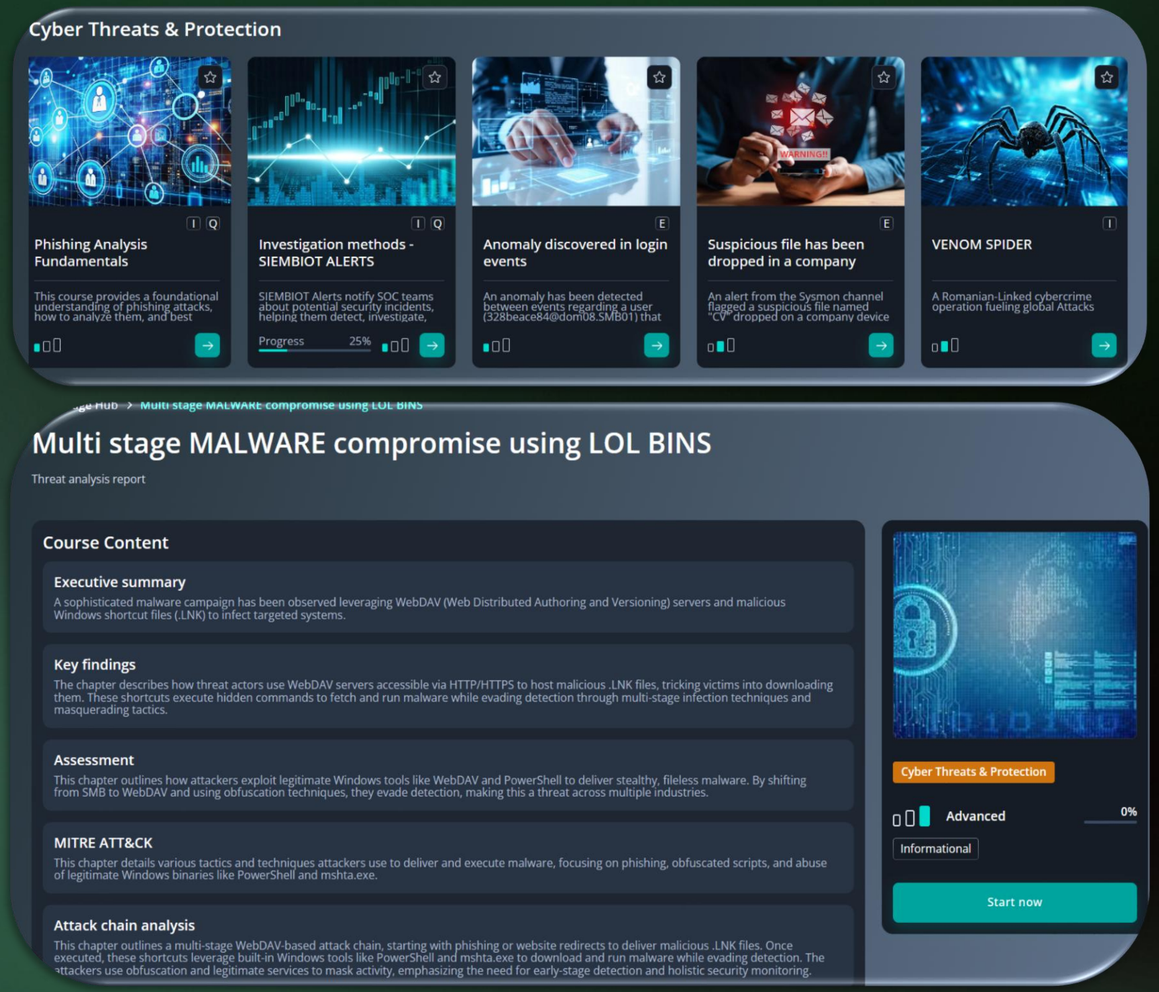
- Email Phishing – Understanding, Preventing, and Responding
- A Beginner's Guide to Online Safety
- Phishing Analysis Fundamentals
- Investigation methods - SIEMBIOT ALERTS
- Anomaly discovered in login events
- Red Team Fundamentals

Nivel: Intermediate, Limba Engleză

- Suspicious file has been dropped in a company
- VENOM SPIDER
- Email header analysis

Nivel: Advanced, Limba Engleză

- Multi stage MALWARE compromise using LOL BINS



Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

De la **Awareness** la competențe **operaționale**

Knowledge Hub

Cunoștințe teoretice

- înțelegerea riscurilor și a amenințărilor
- comportament digital responsabil
- bune practici de securitate
- bază teoretică necesară

Cyber Lab

Aplicare practică

- scenarii inspirate din incidente reale
- analiză și investigare
- lucru în medii simulate SOC (Centrul de Operațiuni de Securitate)
- dezvoltarea competențelor SOC operaționale

Cyber Academy oferă un parcurs educațional complet, de la awareness la competențe operaționale, în linie cu cerințele NIS2.

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Cyber Lab – aplicarea practică a cunoștințelor

- ✓ Testează și analizează **interogări de securitate** pe seturi de date reale.
- ✓ Învață să folosești **DQL (Dashboards QueryLanguage)**, un limbaj simplificat pentru filtrarea și căutarea eficientă a datelor.
- ✓ Explorează o **zonă sigură, unde poți experimenta** liber fără riscul de a afecta sistemul.
- ✓ Vizualizează **date anonimizate în timp real,** colectate de la zeci de mii de dispozitive active.

De unde să începi?

Poți începe cu cursul introductiv din **CyberAcademy – „How to use Cyber Lab”,** care te va ghida pas cu pas în utilizarea laboratorului virtual de securitate cibernetică.

cyber-academy.siembiot.eu/cyber-lab

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

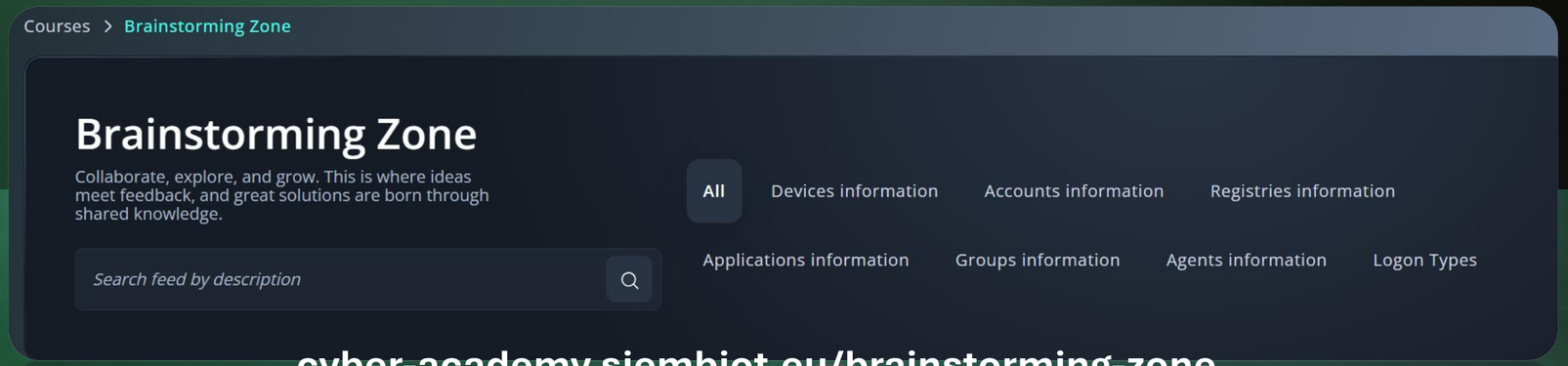
Brainstorming Zone

Colaborare și analiză aplicată

Brainstorming Zone este modulul colaborativ al platformei CyberAcademy, destinat participanților. Este spațiul unde investigațiile individuale din Cyber Lab devin exerciții colective, unde participanții pot discuta scenarii, schimba idei, valida query-uri și colabora pentru a rezolva cazuri de securitate.

Legătura dintre Cyber Lab și Brainstorming Zone este nucleul experienței de învățare:

- Un utilizator care lucrează într-un Playground din Cyber Lab poate deschide direct o discuție în Brainstorming Zone, atașând query-ul sau scenariul investigat
- Alți participanți pot vedea query-ul, îl pot comenta, îmbunătăți sau propune variante alternative
- Discuțiile sunt organizate pe categorii de date (Devices, Accounts, Registries, Applications, Groups, Agents, Logon Types) toate filtrele vizibile în interfața platformei
- Rezultatele colaborării pot fi salvate înapoi ca query-uri în Cyber Lab



cyber-academy.siembiot.eu/brainstorming-zone

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Cyber Academy – Beneficii pentru instituții și organizații

Reducerea riscurilor

✓Reduce riscurile prin îmbunătățirea comportamentului și aplicarea bunelor practici de securitate

Maturitate NIS2

✓Sprijină alinierea la cerințele NIS2 prin dezvoltarea competențelor necesare proceselor și responsabilităților de securitate.

Competențe aplicate

✓Participanții își dezvoltă competențele prin exerciții practice și scenarii inspirate din situații reale.

Aliniere industrie

✓Participanții sunt pregătiți pentru cerințele mediului profesional și pentru procesele utilizate în industrie.

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Demonstrație Practică Cyber LAB

1. Office 365 / OneDrive

Monitorizarea activității utilizatorilor în cloud

- **Query 1 — Custom Mass Download Anomaly:** Detectează toate descărcările unui utilizator specific din OneDrive via SharePoint Online.
- **Query 2 — Events From A Specific IP Address:** Returnează toate evenimentele/operațiunile din Office 365 generate de un IP specific.
- **Query 3 — Events From IP (Excluding OneDrive Downloads):** Similar cu Query 2, dar exclude descărcările din OneDrive — util pentru reducerea zgomotului în investigație.

2. Azure / Risc utilizator

Detectarea comportamentului anormal la autentificare

- **Query 4 — Events Regarding Risk User** Returnează evenimentele Azure legate de risc la autentificare — logon din locație neobișnuită sau nouă, cu generare de alertă pe contul utilizatorului.

3. Sysmon / Process Creation

Investigarea proceselor lansate de browsere

- **Query 5 — Process Creation Generated By Browsers** Toate evenimentele Sysmon Event ID 1 generate de Chrome, Firefox, Opera, Brave.
- **Query 6 — Process Creation — Device specific + URL specific** Rafinează Query 5: returnează procesele create de un browser pe un device anume și pentru un URL specific accesat de utilizator.
- **Query 7 — All Events Containing A Specific Value** Returnează toate evenimentele care conțin un URL specific în context — cel mai simplu mod de a pivota pe un indicator.

4. Investigație avansată (Email + Browser + Outlook)

Corelarea vectorilor de atac

- **Query 8 — Process Creation via Browser, Parent Process = Outlook** Identifică dacă un link suspect dintr-un email Outlook a declanșat un proces în browser, pe un device și URL specifice — **pivot key pentru phishing**.
- **Query 9 — Email Accessed with Specific Subject + Compromised User** Returnează emailurile accesate de utilizatorul compromis care conțin în subiect un cuvânt cheie legat de URL-ul suspect găsit anterior — **închide cercul investigației**.

Toate cele 9 query-uri urmăresc de fapt un singur scenariu de investigație:

1. Se detectează descărcări masive din OneDrive → **Query 1**
2. Se identifică IP-ul sursă și activitatea lui → **Query 2, 3**
3. Se verifică dacă contul este marcat ca risc în Azure → **Query 4**
4. Se caută dacă s-a lansat vreun proces suspect din browser pe device → **Query 5, 6, 7**
5. Se confirmă că procesul a fost declanșat dintr-un email Outlook → **Query 8**
6. Se recuperează emailul original care a inițiat tot lanțul → **Query 9**

Fiecare query nu este izolat, este un pas dintr-o investigație reală end-to-end, exact cum ar lucra un analist SOC.

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Oportunități de colaboare academică și cercetare

Cybersecurity & AI Engineering

1. Programe academice aplicate și laboratoare dedicate

- Dezvoltarea de laboratoare virtuale pentru testare, simulare de atacuri și exerciții de tip cyber range
- Integrarea platformei în curricula / Proiecte practice interdisciplinare

2. Parteneriate pentru cercetare & inovare

- Proiecte comune de cercetare în domenii emergente: AI-driven threat detection, Zero Trust architectures etc.
- Aplicare la granturi europene (Horizon Europe, Digital Europe)
- Publicații științifice și studii de caz bazate pe date reale din industrie

3. Dezvoltarea de centre de excelență

- Crearea unor hub-uri academice în cybersecurity & AI
- Colaborare cu industrie pentru validarea competențelor și alinierea la cerințele pieței

4. Pregătirea viitoarei generații de specialiști

- Internship-uri și programe de mentorat cu experți din industrie
- Proiecte de licență, disertație și doctorat ancorate în provocări reale

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Sesiune Q&A

Co-funded by the European Union

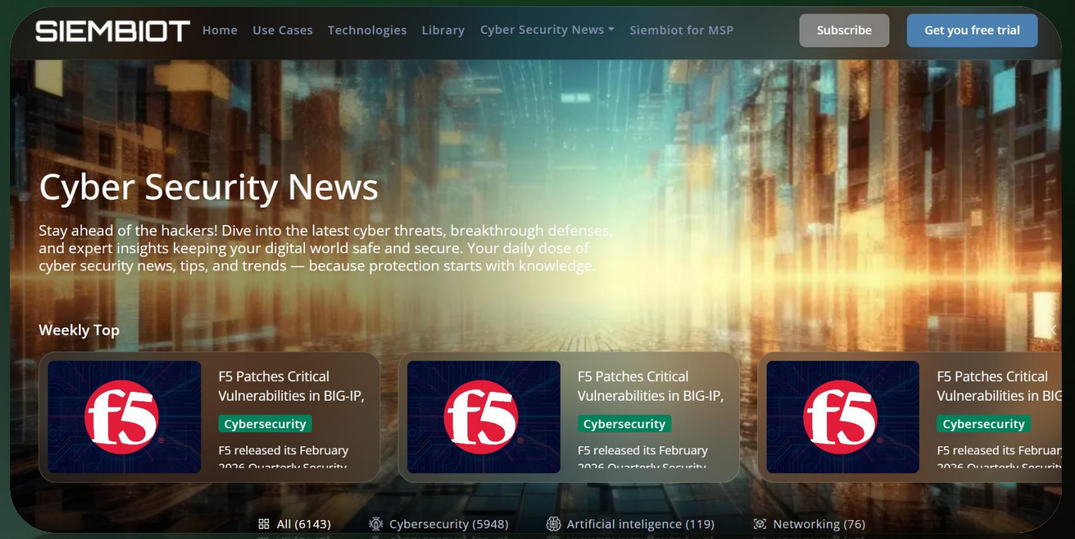
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

Cyber Security News

- ✓ Este **zona stirilor zilnice din Securitate cibernetică** – ce atacuri au loc si cum afecteaza lumea reala.
- ✓ Adună informații de **peste 14 portaluri dedicate securității cibernetice**.
- ✓ Publicam peste **20 de articole săptămânal**.
- ✓ Articole specializate care prezintă în detaliu **incidente reale de securitate**.
- ✓ **Resurse educative explicate simplu** – pentru a înțelege nu doar „ce s-a întâmplat”, ci și „ce putem învăța din asta”



Siembiot.eu/cyber-security-news

Co-funded by the European Union

ECCC EUROPEAN CYBERSEC COMPETENCE CENTRE

Exemple de știri

Expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

15,000 Fake TikTok Shop Domains Deliver

Cybersecurity

Cybersecurity researchers have lifted the veil on a

15.000 de domenii false de magazine TikTok Shop livrează malware și fură criptomonede printr-o campanie de înșelătorie bazată pe inteligență artificială.

Un baraj din Bremanger, Norvegia, a fost sabotat de hackeri pro-ruși, care au eliberat apa timp de patru ore.

Pro-Russian hackers blamed for water dam

Cybersecurity

The Norwegian Police Security Service (PST) says that pro-

North Korea Attacks South Koreans With

Cybersecurity

DPRK hackers are throwing every kind of malware at the

Coreea de Nord este acuzată că a lansat atacuri ransomware asupra unor companii din Coreea de Sud, blocând accesul la date prin criptare și cerând răscumpărare.

La lansarea Battlefield 6, Electronic Arts a identificat și blocat peste 300.000 de încercări de trișare, protejând astfel integritatea jocului online.

Electronic Arts Blocked 300,000 Attempts

Cybersecurity

Electronic Arts has revealed that their Javelin anti-cheat

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

expertware

DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA

expertware

Technology that makes the difference.
Our experts, your solutions.

info@expertware.net

Follow us on:

expertware.net