



SIEMBIOT® CYBER ACADEMY

Platformă educațională pentru dezvoltarea competențelor
în securitate cibernetică

Coordonator

Partener



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

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.

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

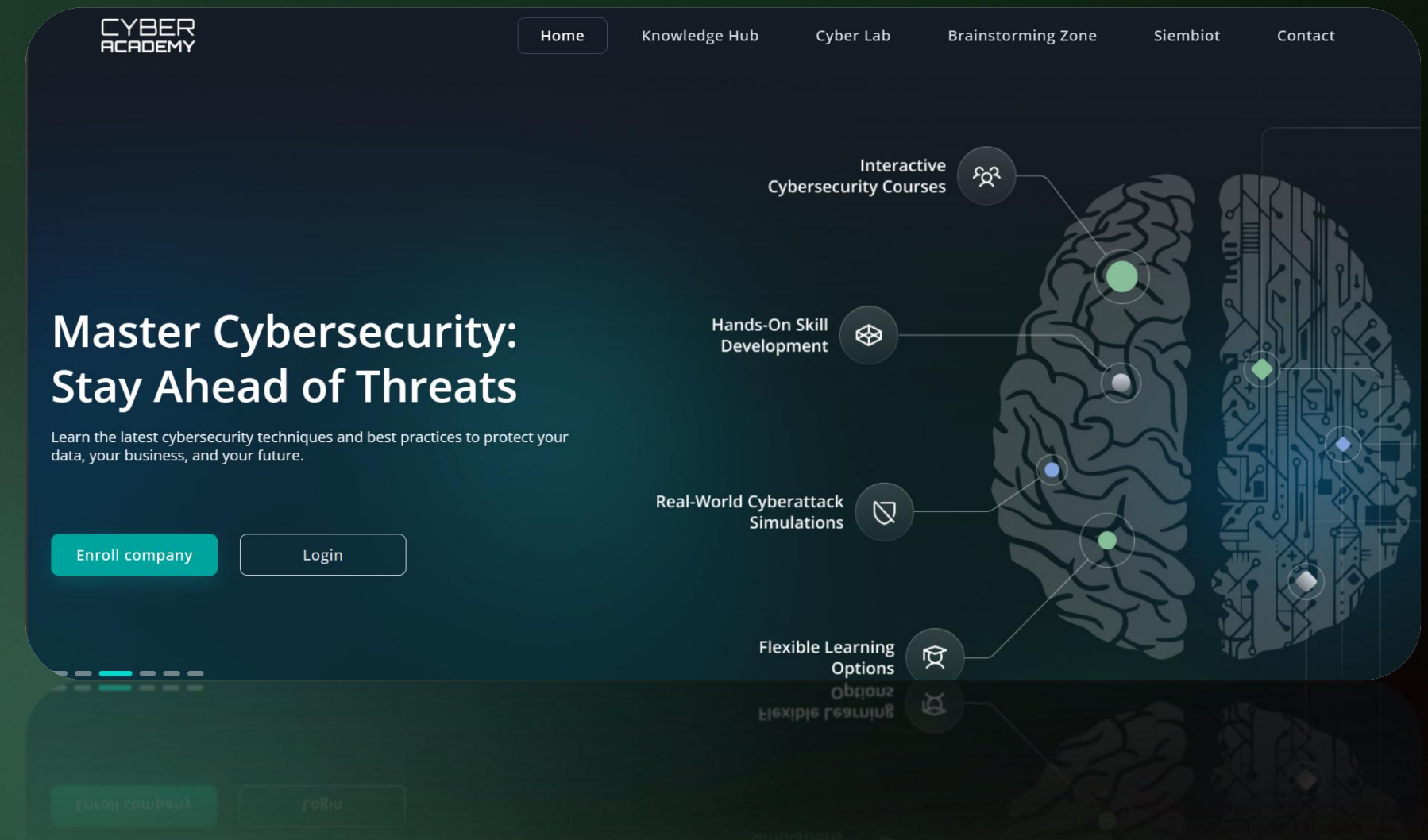
Participanții pornesc de la concepte de bază și ajung treptat la exerciții și scenarii practice.

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/>

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.

BOOST YOUR COMPANY'S SECURITY WITH SOC TRAINING

Equip your SOC team to handle today's toughest cyber threats. Enroll now for expert-led courses tailored for corporate security teams. Build skills, boost defenses, and stay ahead. Start today!

Company name*

Company name

VAT*

VAT

Country*

Select option

Contact person*

Contact person

Contact email*

Contact email

Contact phone number*

Contact phone number

Message

Message

I have reviewed and acknowledged the [Terms and conditions](#) and [Privacy Policy](#) of the Cyber Academy website.

Go to Home

Send request

COMPLETE YOUR REGISTRATION!

You're almost there!

To complete your account setup, please choose a strong password. After you've set your password, you'll gain full access to the courses page, where you can explore all available training resources.

Additionally, you'll be able to invite more attendees from your company to join the courses and enhance their learning experience. We're excited to have you on board!

Username

Nemtoi Marian

Invited by

Test NMM EXP

Password*

Password

Confirm password*

Confirm password

Password requirements

Min 12 characters A-Z a-z 0-9 special characters

I have reviewed and acknowledged the [Terms and conditions](#) and [Privacy Policy](#) of the Cyber Academy website.

Go to Home

Save

Crearea contului

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

Congratulations ACCOUNT REGISTERED



Your account has been successfully registered. You can now log in and start exploring all the features available to you. If you have any questions or need assistance, feel free to contact our support team.

Welcome aboard!

Go to Home

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.

Courses > Administration

Administration

Company name: Test NMM EXP | Company number: 1234 | Country: Romania

Administrators | Students

Search user

Name	Email	Status	Actions
Nemtoi Marian	marian.nemtoi@getronics.com	Approved	

1 result | 10 per page

Invite student

After submission, an invitation email will be sent to the user with instructions on how to proceed. The user will be able to accept the invitation and complete any necessary steps to join the platform.

Name*

Email*

Cancel Save

Administrators | **Students**

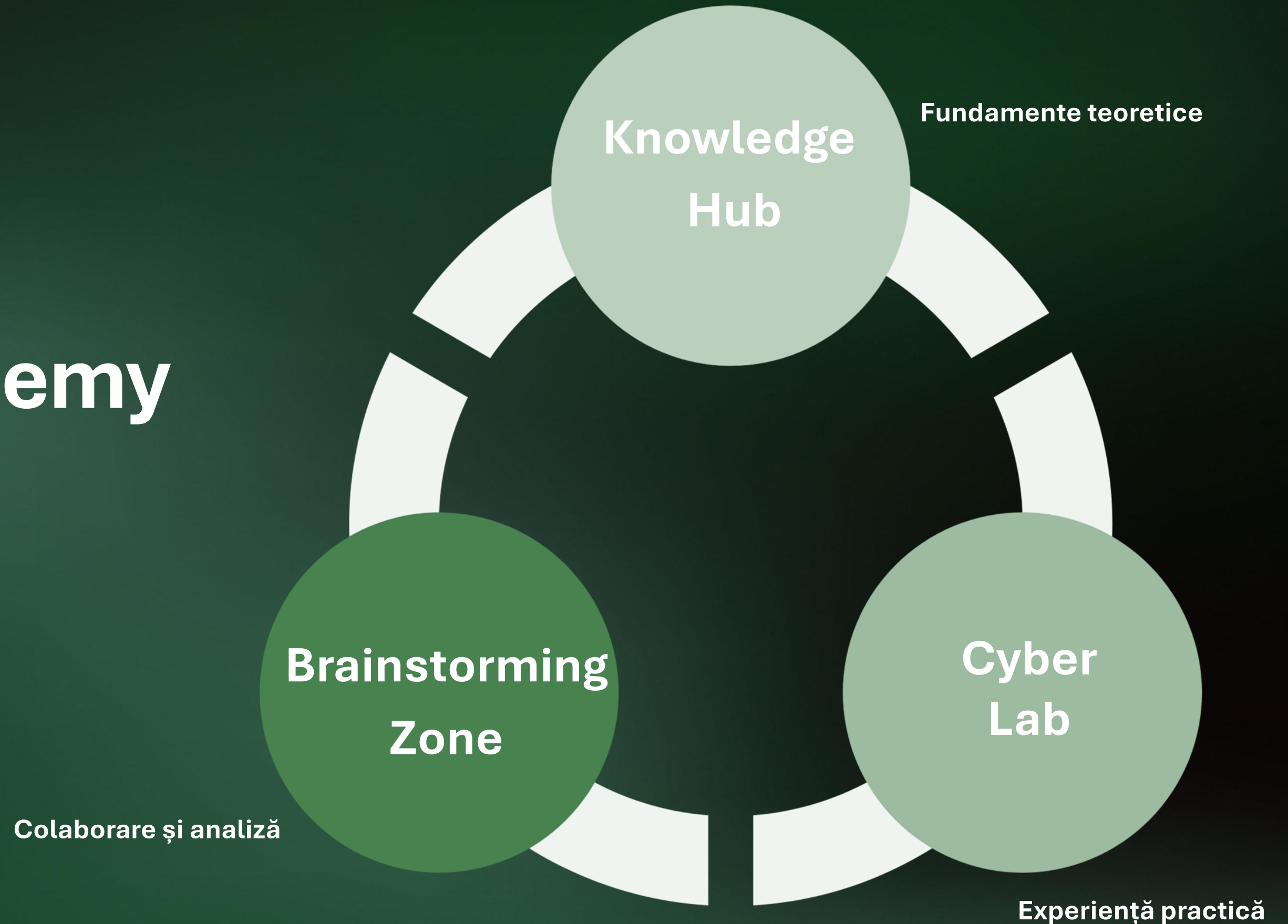
Search user

Search...

Invite student

Name	Email	Started courses	Finished courses	Status	Actions
No content found					

Structură Cyber Academy



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](https://cyber-academy.siembiot.eu/knowledge-hub)






Cybersecurity Standards & Best Practices

 <p>NIST 800-53 Essentials: Unlocking Effective Security</p> <p>NIST 800-53 Essentials: Unlocking Effective Security Controls provides a foundational understanding of</p> <p>Completed</p>	 <p>GDPR in Cybersecurity</p> <p>GDPR in Cybersecurity explores the intersection of data protection and cybersecurity under the General</p>	 <p>Safeguarding Your Network Infrastructure</p> <p>Safeguarding Your Network Infrastructure provides a comprehensive guide to securing</p>	 <p>Cybersecurity Domains and Specializations</p> <p>The discipline of cybersecurity is vast and includes many subfields, each of which focuses on a distinct</p> <p>Completed</p>	 <p>Cyber Security Risk Management - Frameworks</p> <p>In the modern digital landscape, the significance of cybersecurity risk management is more crucial</p>
---	---	---	--	---

Device & Online Security

 <p>Website Cybersecurity: Protecting Your Online</p> <p>Websites are prime targets for cyber threats, from data breaches to hacking attempts. Without</p>	 <p>Securing Your Devices: The Dangers of Leaving Your</p> <p>In this course, you will learn about the security risks associated with leaving your devices unattended</p>	 <p>The Hidden Dangers of Public Wi-Fi: How to Protect</p> <p>Public Wi-Fi networks are convenient but can pose significant cybersecurity risks. Hackers often</p> <p>Progress 20%</p>	 <p>Cybersecurity in Mobile Banking: Protecting Your</p> <p>Mobile banking has become a convenient way to manage finances, but it also presents</p>	 <p>The Importance of Device Security & Updates</p> <p>In today's interconnected world, the security of your devices is more important than ever. This course</p>
---	--	---	--	--

Cyber Threats & Protection

 <p>Email Phishing - Understanding, Preventing, and Responding</p> <p>Email Phishing - Understanding, Preventing, and Responding provides essential knowledge on</p>	 <p>A Beginner's Guide to Online Safety</p> <p>This course provides essential knowledge to help you navigate the digital world securely. You will learn</p>	 <p>Phishing Analysis Fundamentals</p> <p>This course provides a foundational understanding of phishing attacks, how to analyze them, and best</p>	 <p>Investigation methods - SIEMBIOT ALERTS</p> <p>SIEMBIOT Alerts notify SOC teams about potential security incidents, helping them detect, investigate,</p> <p>Progress 25%</p>	 <p>Anomaly discovered in login events</p> <p>An anomaly has been detected between events regarding a user (328beace84@dom08.SM/B01) that</p>
--	---	--	---	---

Structura unui curs în Cyber Academy

The screenshot shows a course page with the title 'Cybersecurity Domains and Specializations'. It includes a 'Beginner' difficulty level, a 'Cybersecurity Standards & Best Practices' tag, and a description of the discipline. Below the main content, there are sub-topics: 'Network Security, Endpoint Security, and Cloud Security'. The page also features a 'Quiz' button and a 'Knowledge Hub' navigation menu.

- ✓ 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.

The screenshot shows a quiz question: 'Q1: Which of the following are key components of network security?'. The options are: A) Firewalls, B) Intrusion Detection and Prevention Systems (IDPS), C) Social media tracking, and D) Virtual Private Networks (VPNs). Each option has a checkbox next to it.

The screenshot shows a course page for 'Incident Response Lifecycle'. It includes a circular diagram with six stages: Preparation, Detection/Analysis, Containment, Eradication, Recovery, and Post-Incident. The diagram is surrounded by text describing the lifecycle and a list of 'Typical Problems in Incident Response'. On the right side, there is a 'Course Chapters' list with four items, each marked with a checkmark: 'Network Security, Endpoint Security, and Cloud Security', 'IAM, or identity and access management', 'DevSecOps and Application Security', and 'Incident Response and the Security Operations Centre (SOC)'. The page also features a 'Quiz' button and a 'Knowledge Hub' navigation menu.

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)**

Cybersecurity Standards & Best Practices



The screenshot displays a grid of four course cards. Each card features a representative image, a title, a brief description, and a progress indicator. The first card, 'NIST 800-53 Essentials: Unlocking Effective Security', shows a person at a computer workstation and is marked as 'Completed'. The other three cards, 'GDPR in Cybersecurity', 'Safeguarding Your Network Infrastructure', and 'Cybersecurity Domains and Specializations', show various network and security-related graphics. Each card includes a star icon for favorites and a right-pointing arrow for navigation.

Cursuri de Device & Online Security

Nivel: Beginner, Limba Engleză

Device & Online Security

- Website Cybersecurity: Protecting Your Online**
Websites are prime targets for cyber threats, from data breaches to hacking attempts. Without
- Securing Your Devices: The Dangers of Leaving Your**
In this course, you will learn about the security risks associated with leaving your devices unattended
- The Hidden Dangers of Public Wi-Fi: How to Protect**
Public Wi-Fi networks are convenient but can pose significant cybersecurity risks. Hackers often
- Cybersecurity in Mobile Banking: Protecting Your**
Mobile banking has become a convenient way to manage finances, but it also presents
- The Importance of Device Security & Updates**
In today's interconnected world, the security of your devices is more important than ever. This course

Securing Your Devices: The Dangers of Leaving Your Devices Unattended

In this course, you will learn about the security risks associated with leaving your devices unattended and how cybercriminals exploit these opportunities. We will explore real-world threats such as unauthorized access, data theft, malware installation, and physical tampering. You will also discover best practices for securing laptops, smartphones, and other devices in public and private spaces.

Course Content

Introduction to Device Security

Device security is the first line of defense against cybercriminals and unauthorized access. This chapter introduces the fundamental concept of device security and outlines why it's critical to secure your devices, especially when they are not in use. We'll explore how the smallest oversight, like leaving your device unlocked for just a few minutes, can open the door for thieves, hackers, or malicious actors to exploit vulnerabilities.

The Dangers of Physical Theft and Unauthorized Access

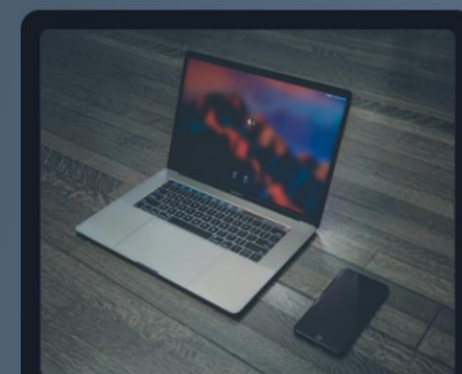
This chapter dives into the direct risks associated with leaving devices physically unattended. We'll look at how easy it is for devices like laptops, smartphones, and tablets to be stolen when left unsecured in public or at home. Physical theft is one of the easiest ways cybercriminals gain access to personal data. But theft is just one part of the story. Unauthorized access can also occur when a device is left unlocked or unattended in shared or unsecured spaces.

Protecting Personal Data from Cyber Criminals

In today's digital age, personal data is a valuable commodity. Cybercriminals are constantly looking for ways to steal information such as passwords, financial records, and personal files, especially from devices that are left unattended. In this chapter, we'll examine the types of cyberattacks that can occur when your device is not properly secured, including phishing, social engineering, spyware, and keylogging.

Best Practices for Locking and Securing Your Devices

This chapter provides practical, actionable steps you can take to secure your devices. It goes beyond theory and gives you clear, step-by-step instructions for locking down your devices, making sure they're safe from unauthorized access. A secure device is one that requires authentication before it can be accessed, whether through a PIN, password, fingerprint, or facial recognition.



Device & Online Security

Beginner

0%

Informational

Quizzes

Start now

- 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

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

Cyber Threats & Protection

- Phishing Analysis Fundamentals
- Investigation methods - SIEMBIOT ALERTS
- Anomaly discovered in login events
- Suspicious file has been dropped in a company
- VENOM SPIDER

Multi stage MALWARE compromise using LOL BINS

Threat analysis report

Course Content

Executive summary
A sophisticated malware campaign has been observed leveraging WebDAV (Web Distributed Authoring and Versioning) servers and malicious Windows shortcut files (.LNK) to infect targeted systems.

Key findings
The chapter describes how threat actors use WebDAV servers accessible via HTTP/HTTPS to host malicious .LNK files, tricking victims into downloading them. These shortcuts execute hidden commands to fetch and run malware while evading detection through multi-stage infection techniques and masquerading tactics.

Assessment
This chapter outlines how attackers exploit legitimate Windows tools like WebDAV and PowerShell to deliver stealthy, fileless malware. By shifting from SMB to WebDAV and using obfuscation techniques, they evade detection, making this a threat across multiple industries.

MITRE ATT&CK
This chapter details various tactics and techniques attackers use to deliver and execute malware, focusing on phishing, obfuscated scripts, and abuse of legitimate Windows binaries like PowerShell and mshta.exe.

Attack chain analysis
This chapter outlines a multi-stage WebDAV-based attack chain, starting with phishing or website redirects to deliver malicious .LNK files. Once executed, these shortcuts leverage built-in Windows tools like PowerShell and mshta.exe to download and run malware while evading detection. The attackers use obfuscation and legitimate services to mask activity, emphasizing the need for early-stage detection and holistic security monitoring.

Cyber Threats & Protection

Advanced 0%

Informational

Start now

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

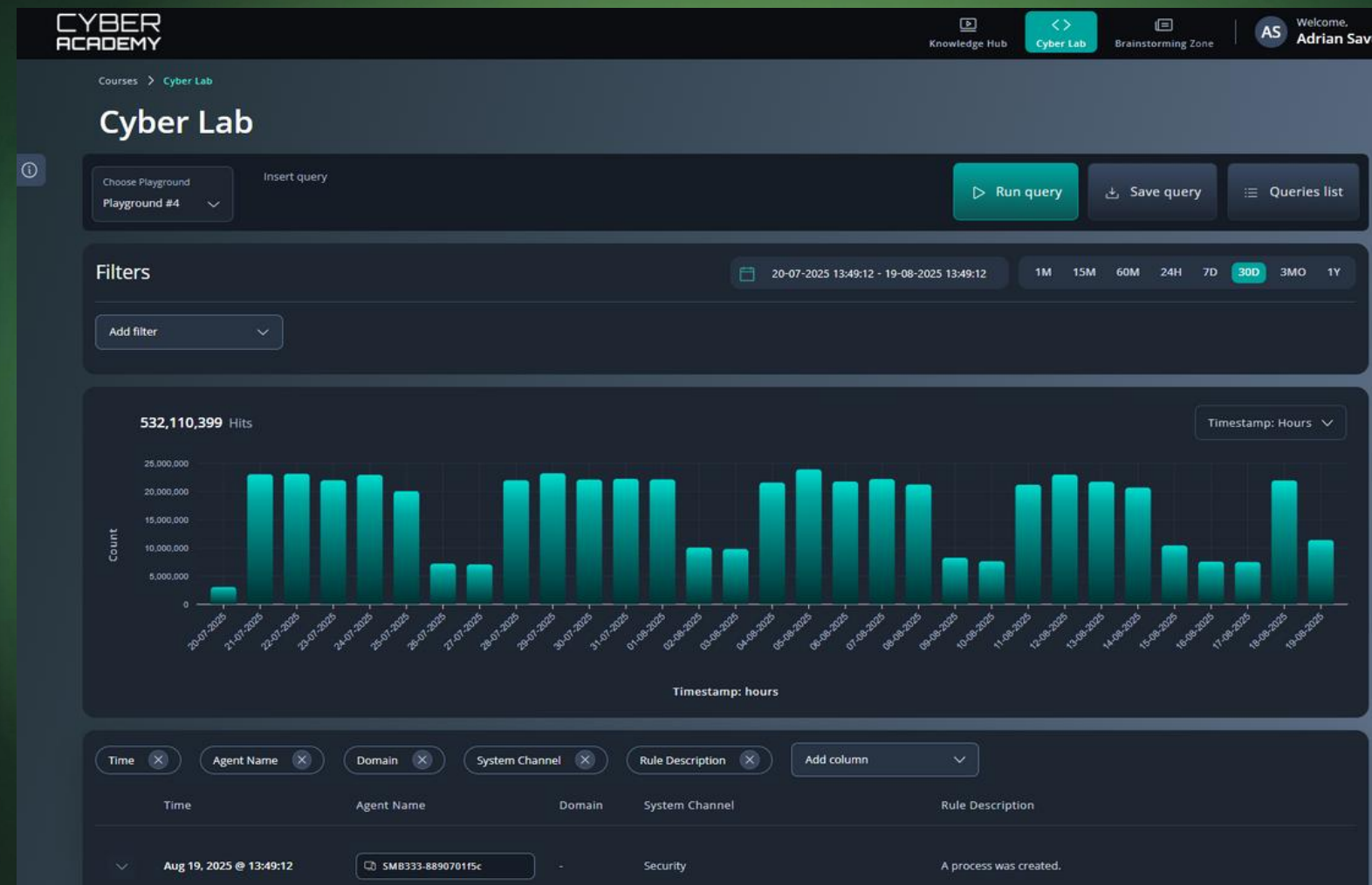
Cyber Lab

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.

Cyber Lab – aplicarea practică a cunoștințelor



- ✓ Testează și analizează **interogări de securitate** pe seturi de date reale.
- ✓ Învăț 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

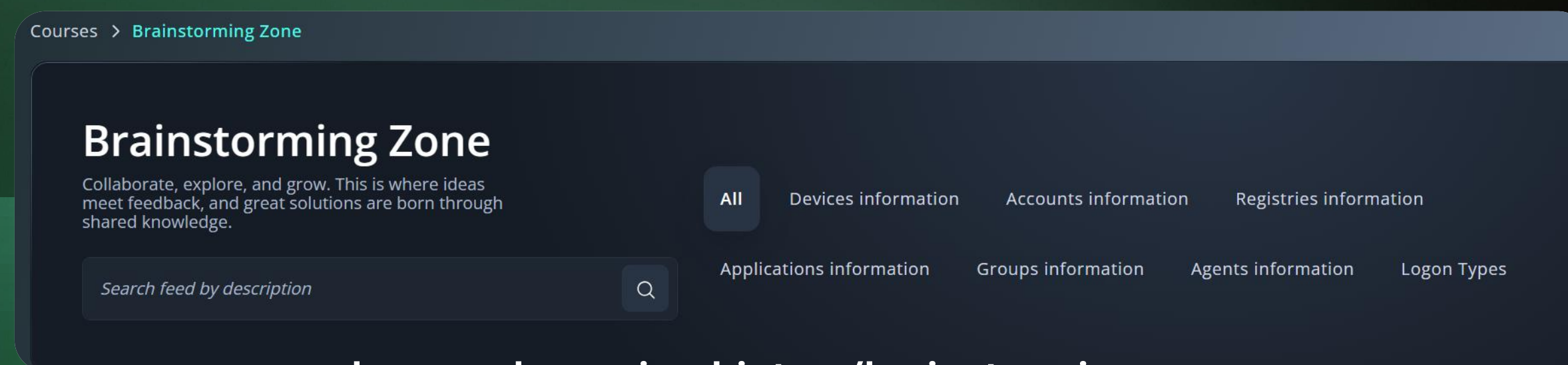
Brainstorming Zone

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

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.

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.

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

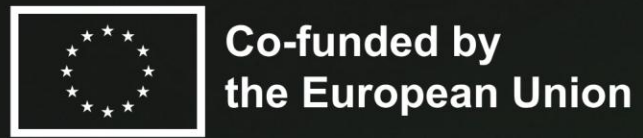
- Proiecte comune de cercetare în domenii emergente: AI-driven threat detection, Zero Trust architectures etc.
- Aplicare la granturi europene (Horizon Europe, Digital Europe)
- Publicații științifice și studii de caz bazate pe date reale din industrie

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

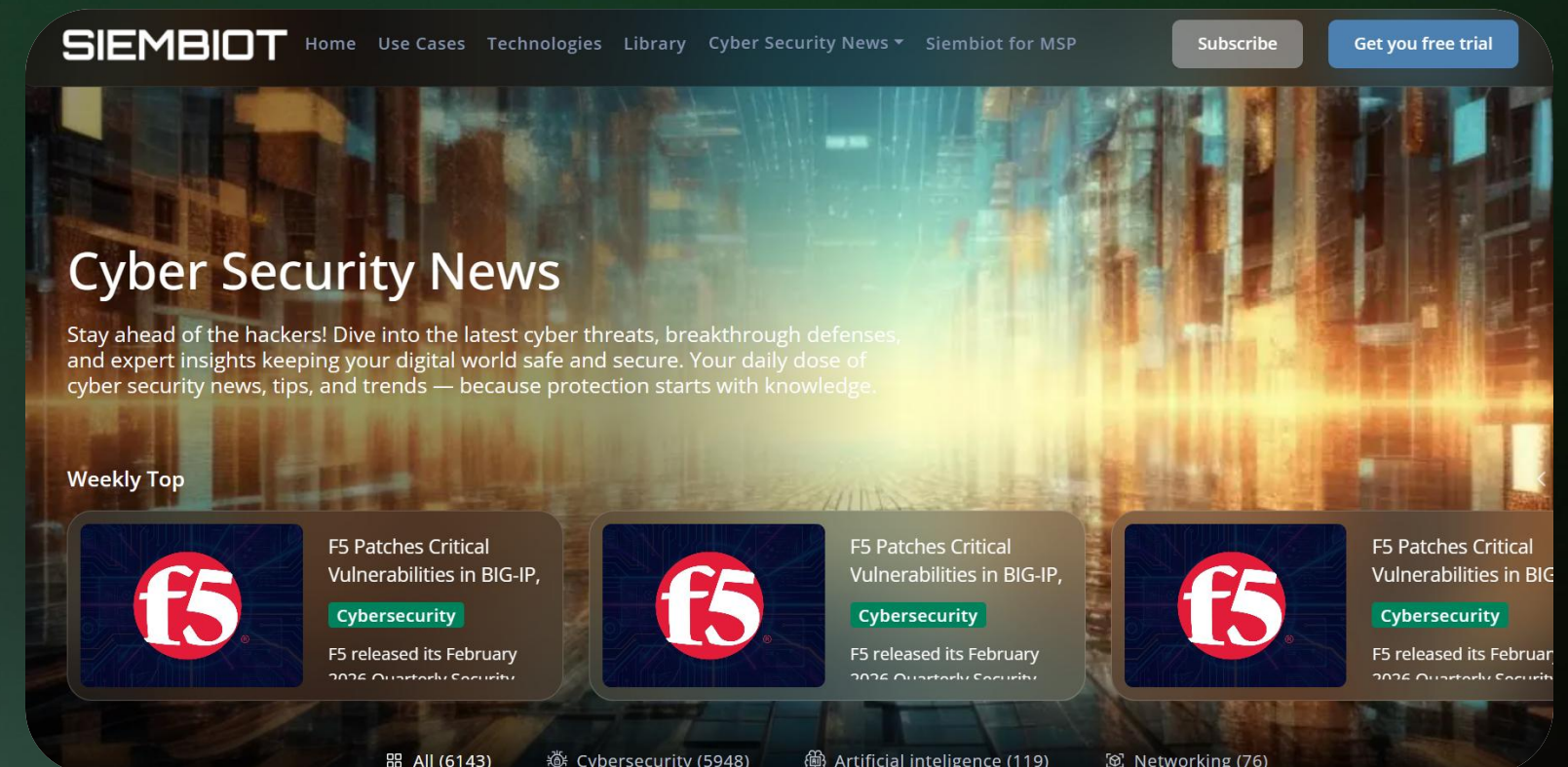


Sesiune Q&A

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 cibernetică**.
- ✓ 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](https://siembiot.eu/cyber-security-news)





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.

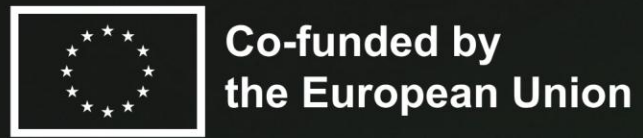
La lansarea Battlefield
6, Electronic Arts a
identificat și blocat
peste 300.000 de
încercări de trișare,
protejând astfel
integritatea jocului
online.



Electronic Arts Blocked
300,000 Attempts

Cybersecurity

Electronic Arts has revealed
that their Javelin anti-cheat



e^xpertware

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



info@expertware.net

Follow us on:

