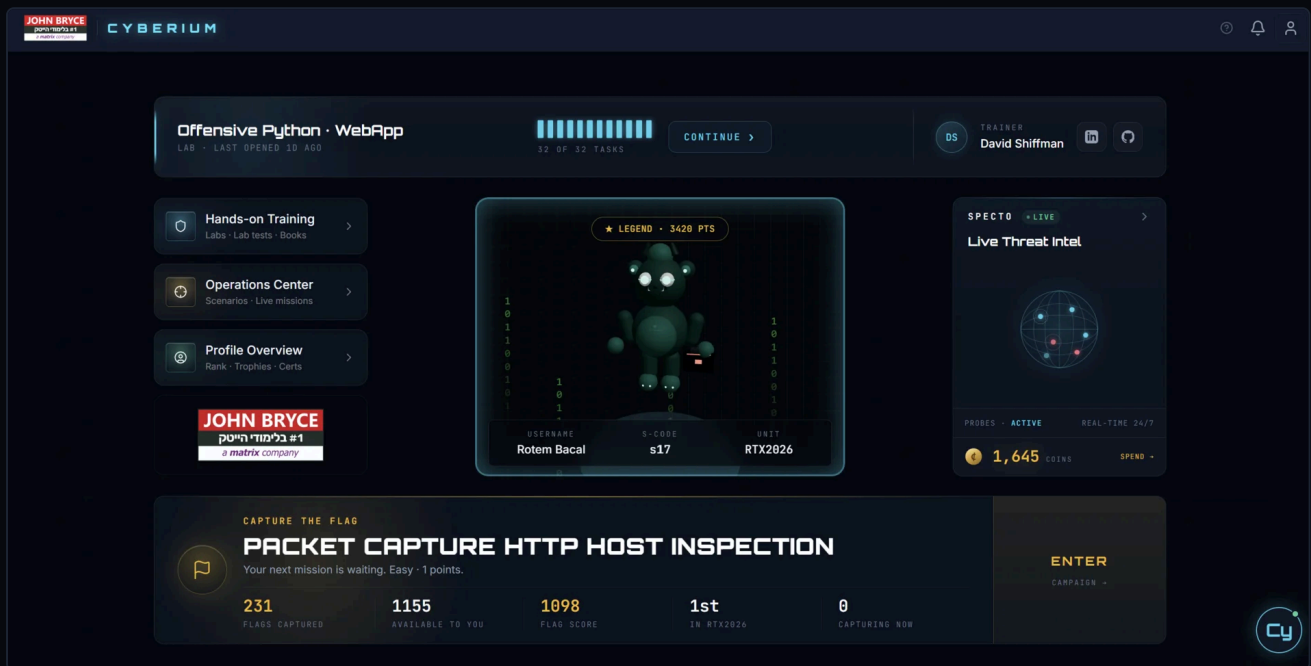


A training centre you never had to build.

Organisations that want cyber training inside their own walls stall at the same place: the curriculum, the lab, the instructors and the assessment are four separate projects, and none of them is the one you do for a living. Cyberium Arena is all four, already built, running under your own name.



WHAT A STUDENT OPENS · A PARTNER'S OWN BRANDING, THE LAB THEY LEFT YESTERDAY, RANK, LIVE THREAT FEED AND THE NEXT FLAG WAITING

They learn the job by doing the job

A student opens a terminal into a real system and is given something to find. Not a video, not a quiz with four answers. The machine behaves the way a machine behaves, including when they get it wrong – which is the part that teaches.

Everything runs in the browser, on whatever machines your people already have in front of them.

Nothing to install. Nothing for your IT department to approve.

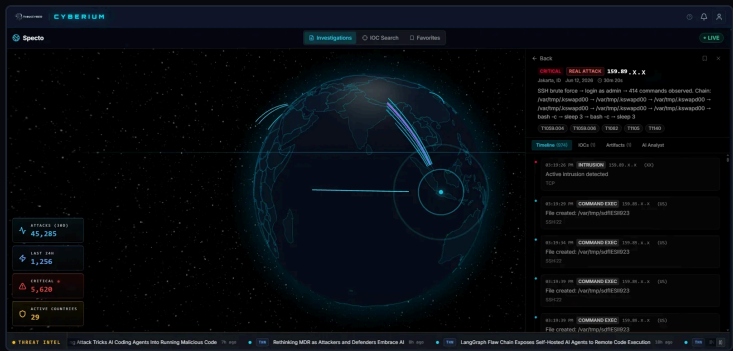


LIVE SCENARIO · THE STUDENT'S TERMINAL

Real attacks, not invented ones

Specto is our live threat feed, and it runs inside the platform. What your students look at is traffic captured on live sensors – the intrusion, the commands the attacker actually ran, and the technique behind each one.

It is the difference between teaching what an attack looks like and showing one that happened this morning. Source addresses are masked; everything else is what we saw.



SPECTO · A CAPTURED INTRUSION, OPENED

You run it. Not us.

Your instructors launch scenarios, watch them play out, and stop or extend them as the session needs, with every seat in the room visible at once. Every exercise is recorded against the person who did it, so “is this working” is answered from the screen rather than from an impression.



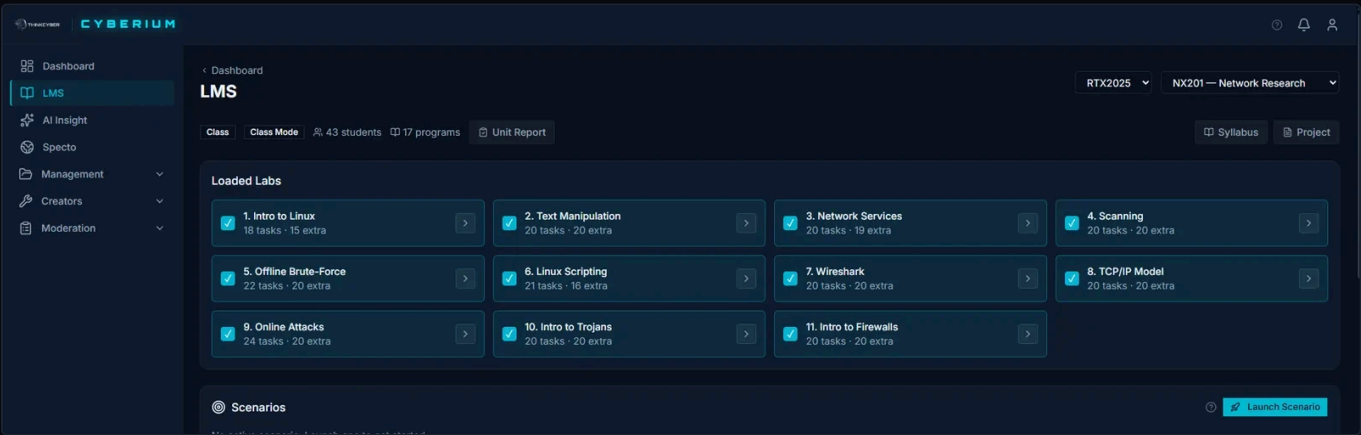
OPERATOR VIEW · RUNNING A SCENARIO

- 01

Runs under your name
Your own space, carrying your logo. Every screenshot in this document is a partner’s – their students see them, not us.
- 02

Open within 24 hours of your details
No hardware, no installation, no instructor certification to complete first. We open your space and import your people from a spreadsheet.
- 03

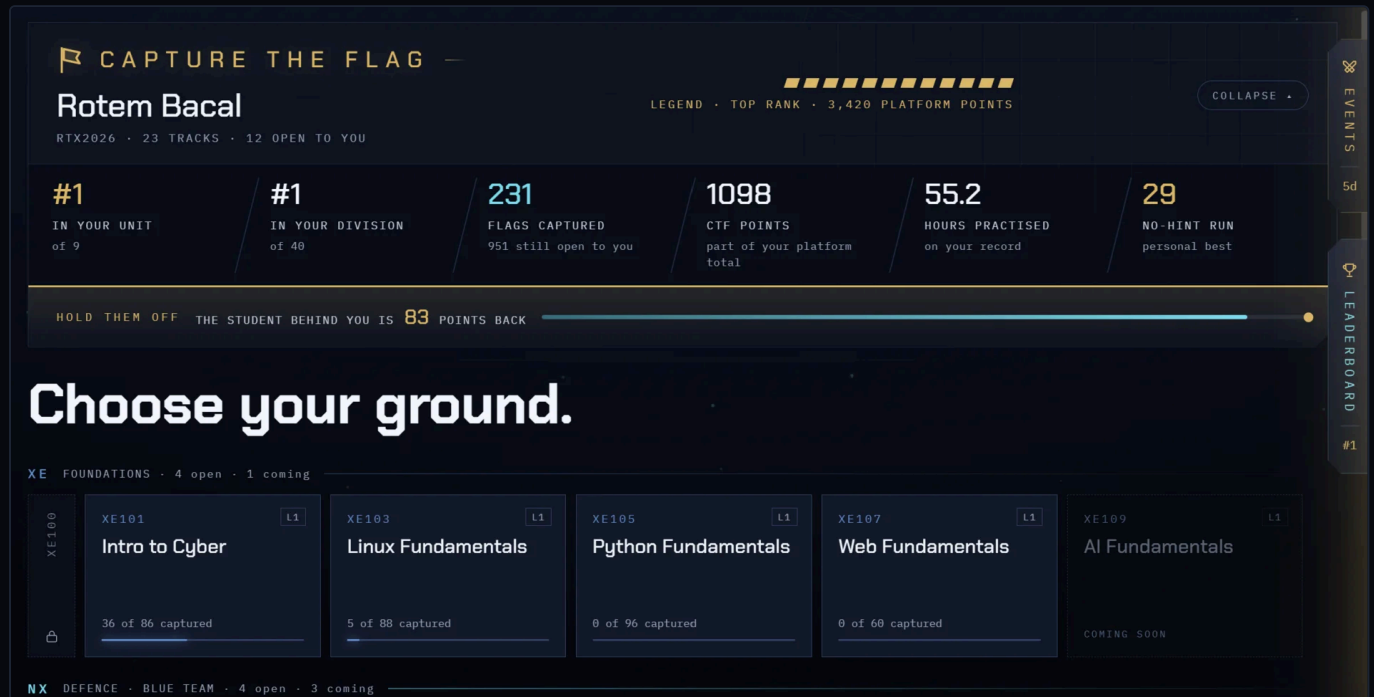
Built by people who did the work
The material comes out of Israeli military and national cyber practice, not a textbook.



TRAINER VIEW · CLASSES AND MODULES

The easiest thing to put in front of a new class.

No lecture, no lesson plan. You put a group in front of it and they compete. It is usually how an organisation finds out which of its own people have the instinct for this work — worth knowing before a budget is spent on them.



FIRST IN THEIR UNIT AND THEIR DIVISION · 231 FLAGS CAPTURED, 951 STILL OPEN, AND 83 POINTS BETWEEN THEM AND THE STUDENT BEHIND

The next step is not a presentation. It is putting a real class on the platform and watching what they do with it.

The catalogue is not the syllabus

These are building blocks. A programme can be assembled from material across tracks and levels and delivered as one course under your own name — so what your people study is the role you are training them for, rather than the course that happens to exist. Most organisations start from a track and then change it.

Every programme, and the level it sits at.

One numbering runs across all four tracks, from a first day with no background at level one to exploit development and industrial control at level seven. A student does not restart when they change direction – they carry their level with them.

XE Foundations

Assumes no background.

1 XE100
Security Awareness

1 XE101
Intro to Cyber

1 XE103
Linux Fundamentals

1 XE105
Python Fundamentals

1 XE107
Web Fundamentals

1 XE109
AI Fundamentals

ZX Offensive security

Attack technique, taught so defenders understand it.

3 ZX301
Penetration Testing

4 ZX305
Network Security

5 ZX322
Offensive Python

6 ZX310
Cyber Warfare

6 ZX311
WebApp Security

6 ZX327
Offensive Linux

7 ZX331
Exploit Development

NX Defence & forensics

The work of a security operations team.

2 NX201
Network Research

3 NX212
Windows Forensics

3 NX220
SOC Analyst

4 NX224
SOC AI

4 NX215
Linux Forensics

4 NX216
Network Forensics

5 NX214
OSINT

6 NX232
Malware Analysis

CX Industrial & ICS

Where the risk is physical as well as digital.

7 CX401
ICS & OT Fundamentals

7 CX410
OT/ICS Security Assessment