ABOSS

Cybersecurity Laboratory
Built, secured, operated · Live in production

A production-grade cyber range for your institution.

Students run real attack-and-defend exercises from any browser. Nothing to install, nothing exposed, and every class starts clean.

ABOSS designs, deploys, secures and operates a complete hands-on cybersecurity lab — dozens of isolated offensive and defensive systems behind one encrypted front door, single sign-on through your existing accounts, continuous monitoring and an automated nightly reset. Built for colleges, training institutes and enterprise security teams: your faculty teaches on it, ABOSS runs it.

range status	operational
front door	tls active
identity	sso federated
segmentation	enforced
ids sensors	reporting
public exposure	none
nightly reset	scheduled

- Live in production
- Browser-based access
- Single sign-on
- Segmented & monitored
- Nightly reset

What the lab gives your learners

Browser-based access	Terminal and remote-desktop sessions to every lab machine open in a tab, through one institutional login. No client software, no VPN, no per-system passwords.
Offensive & defensive systems	Attacker workstations, deliberately vulnerable hosts and web apps, a Windows Active Directory environment, malware-analysis tooling and full blue-team monitoring stacks.
Challenge & scoring platform	Flag submission, scoring and a live leaderboard, with a per-learner instance so every student gets an independent target.
Clean start, real telemetry	Nightly reset to a known-good baseline with on-demand restore, plus network and host intrusion-detection sensors feeding genuine data to defensive exercises.

How it is built — one secure door in, eyes on everything

01	**Secure web layer**	Hardened reverse proxy · HTTPS/TLS · one address · nothing internal exposed
02	**Identity layer**	Single sign-on broker · federated to your accounts · short-lived sessions
03	**Application services**	Remote-access gateway · challenge platform · training web apps, containerised
04	**Lab target systems**	Attacker workstations · vulnerable hosts · Windows AD · analysis tooling, segmented

monitoring spans every layer

Contained by design
Attack traffic stays inside the range, never on the campus network

Least exposure
One encrypted entry point; internal systems never published directly

No standing credentials
Short-lived sessions with time- and class-based access

Validated before go-live
Every path and identity flow verified, then remediated

What ABOSS delivers

- The full range: gateway, challenge platform, training apps and target systems
- SSO federated to your identity provider, TLS everywhere with auto-renewal
- Segmentation, intrusion detection, alerting and automated daily health reporting
- Nightly reset automation and security validation before go-live
- Cut-over to your production domain and institutional branding
- **Ongoing operation** — monitoring, recovery and maintenance handled by ABOSS

Platform & deployment

Infrastructure	Linux virtualisation · Nginx reverse proxy · Docker · segmented networking
Security	TLS auto-renewal · SSO / federated identity · network & host IDS · SIEM · firewall controls
Operations	Git-managed configuration · scheduled automation · CI/CD-ready
Runs on	Your own right-sized hardware, or AWS · GCP · DigitalOcean · Linode — same architecture
Roadmap	Self-hosted AI/LLM serving on your compute for AI-assisted security coursework

How the engagement runs

01	02	03	04	05
Discover	**Design**	**Build & secure**	**Automate & test**	**Deploy & operate**
Map curriculum needs to systems and access patterns	Segmented architecture, one front door, central identity	Provision, containerise, TLS, SSO, isolation	Nightly reset, health reporting, validation	Live on your domain; ABOSS runs it day to day

What changes for your institution

Many risky, hard-to-manage systems **One consolidated, professionally operated platform**	Install-heavy access, separate logins **Any browser, one institutional login**
Vulnerable systems near the campus network **Segmented, contained lab environment**	Manual recovery after a class breaks something **Automated nightly reset, restore on demand**
Limited visibility into what happened **Continuous monitoring, alerting, daily reporting**	Uncontrolled infrastructure cost **Right-sized infrastructure, no always-on cloud bill**

Have a lab or platform that needs to be built, secured, deployed and operated properly?

Let's build the infrastructure behind it. We build to strong, honest security standards — we don't promise "100% secure", because no one credible does.

+91 73973 93006
enquiry@aboss.tech
aboss.tech/solutions/cybersecurity-lab

Book a consultation
aboss.tech/demo