PlayCISO

FOR PLAYERS

Warm up before the flags go live.

Sharpen the blue-team skills a CTF leans on. Each lab runs in the browser on synthetic data and scores your decisions.

- **PCAP Analysis Lab**
  Safe, synthetic packet captures with guided questions, Wireshark-style filters, statistics and debriefs.
- **Detection Lab**
  SIEM detection tickets across Windows, Sysmon, Linux, CloudTrail, proxy and EDR logs.
- **SOC Log Triage Trainer**
  Spot the bad entries in a stream of 1,000 synthetic logs from across the enterprise stack.
- **SOC Case Triage**
  Set the priority from P1 to P4, assign the right team and choose the first action.
- **Email Auth Lab**
  SPF, DKIM and DMARC tickets: fix the 10-lookup limit, rotate DKIM, ramp to p=reject.
- **Leak-Forum CTI Lab**
  Correlate synthetic leak-forum posts to spot a recycled breach or an alias linkage.
- **Firewall Lab**
  Clean up an inherited ruleset, write least-privilege rules and contain a compromised host.

After the flags: lead the incident

The Cyber War Room puts you in charge of the response to a branching incident. A free account includes 3 campaigns.

PlayCISO labs are practice, not a CTF and not an accredited qualification. A free account includes 3 runs across tools and labs and 3 Cyber War Room campaigns. Downloads and exports come with Pro.