

SID 2025

Sibiu Innovation Days

06-07 November, Sibiu - RO



**CHRONOS
SECURITY**

×

MIRACHRON



MARIN Radu

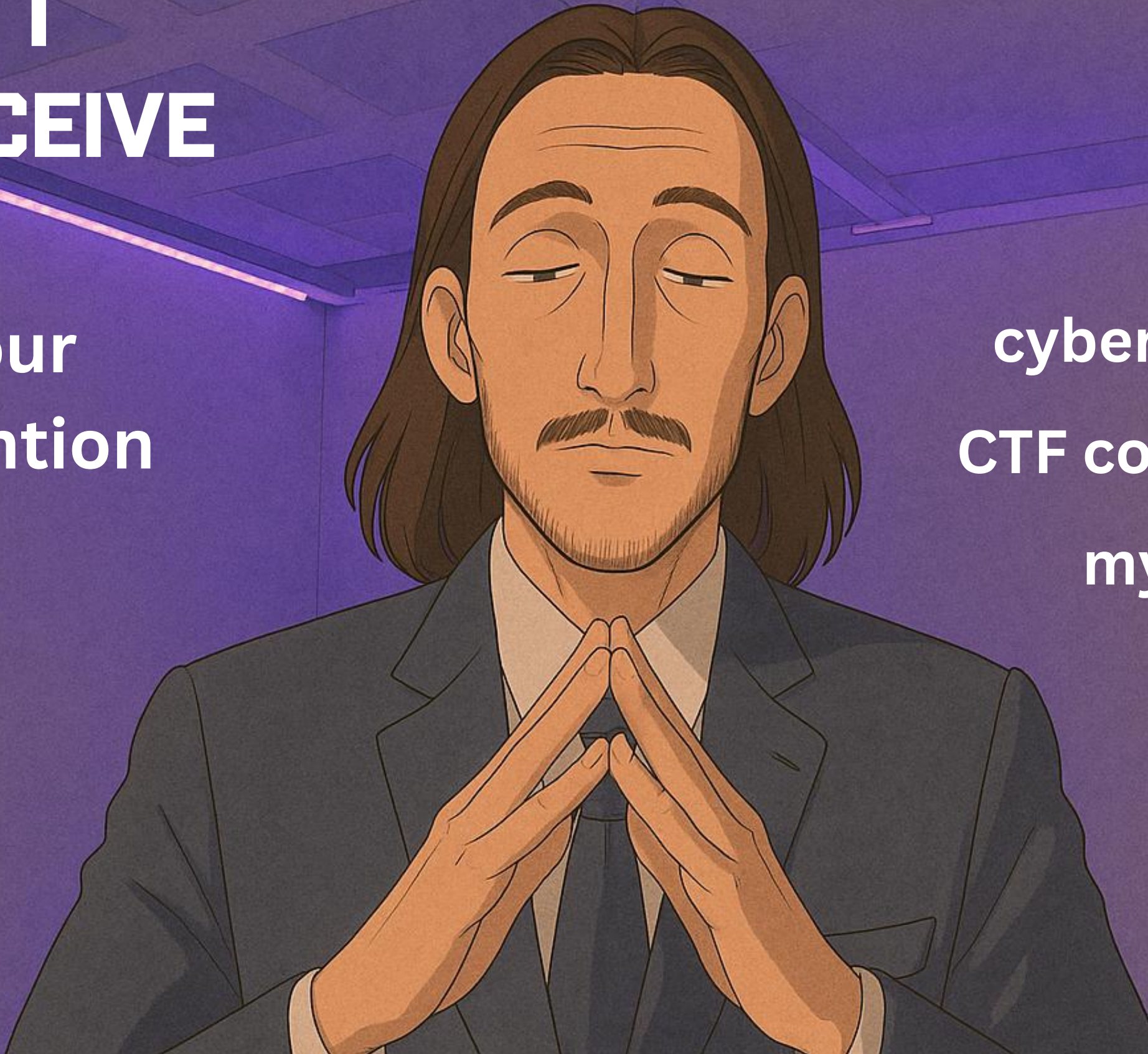
**Evidence-Based Cyber Education:
CTFs, Labs, and Real-World Readiness**

**I
RECEIVE**

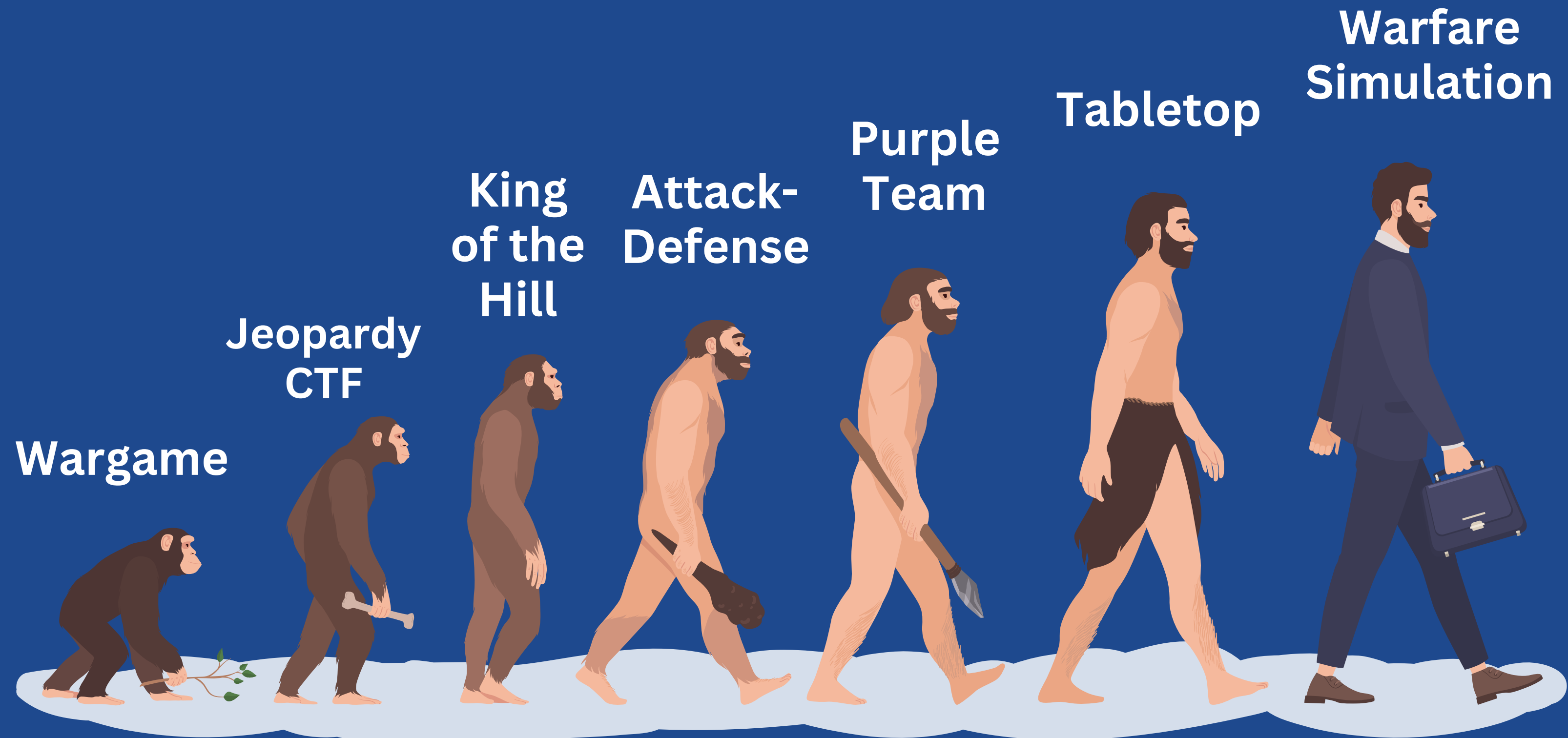
**Your
attention**

**YOU
RECEIVE**

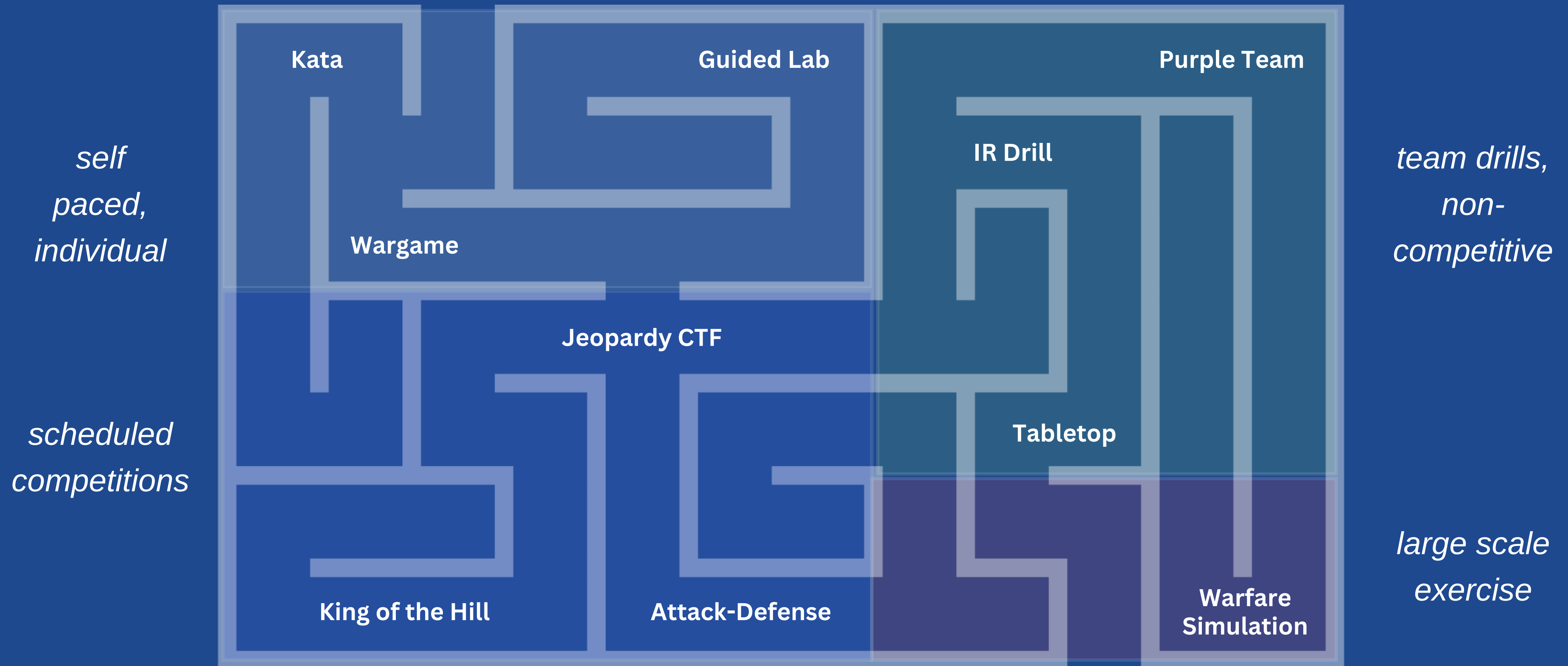
**cyber training categories
CTF competitions analysis
my unsolicited advice**



Cybersecurity training categories



Cybersecurity training categories



Cybersecurity training categories

0. Template

	Outcome	
	Session flow	 Upsides
	What it is	
	Problem solved	
	Who it's for	 Downsides
	Feedback	

EXAMPLES




EXAMPLES

EXAMPLES

Cybersecurity training categories

0. Template

	Teamwork	★ ★ ★ ★ ★
	Difficulty	★ ★ ★ ★ ★
	Setup	★ ★ ★ ★ ★
	Realism	★ ★ ★ ★ ★
	Ops-Pressure	★ ★ ★ ★ ★

	Preparation:
	Execution:
	Verify:

EXAMPLES







EXAMPLES



EXAMPLES

Cybersecurity training categories

1. Kata

a method, not a platform

-  Make critical actions automatic
-  Sample → Steps → Verify → Record
-  Short, fixed drill + repeat
-  Slow, error-prone tasks
-  New analysts; teams standardizing
-  Instant feedback → checklist + time

-  Fast measurable gains
Self-paced
Guided
-  Narrow scope
Can be rote
Low creativity

Cybersecurity training categories

1. Kata



Teamwork



Difficulty



Setup



Realism



Ops-Pressure



Preparation: same day











Execution: 10-20 mins

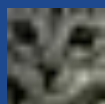


Verify: time, errors, completeness

Cybersecurity training categories






2.1. Wargame - Offensive

- | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p> Attack fluency through discovery</p> <p> Scope → Enumerate → Exploit → Escalate → Prove</p> <p> Unguided target; unknown path to flag</p> <p> Bridge theory to hands-on exploitation</p> <p> Aspiring pentesters / red teamers</p> <p> Instant → flag/proof + timer</p> | <p> Real tools, real tradecraft
Fast wins, high retention
Wide vulnerability coverage</p> <p> Contrived bugs; habit risk
Solo mode; weak teamwork
Low ops/process realism</p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



Cybersecurity training categories

2.1. Wargame - Offensive

	Teamwork	★		Preparation: 1-7 days
	Difficulty	★★★★		Execution: 30-120 min per target
	Setup	★★		Verify: flag + writeup + time-to-exploit
	Realism	★★		
	Ops-Pressure	★		



Cybersecurity training categories

2.2. Wargame - Defensive

① Investigation-to-explanation mastery

👉 Triage → Pivot → Prove → Report

? Self-paced artifact case (logs/pcap/mem)

⚠️ Turn data into evidence fast

👤 SOC analysts • Threat hunters • DFIR juniors

👍 Instant • rubric/answer key











Realistic telemetry slices
Teaches repeatable workflow
Reusable practice cases



Dataset overfit risk
Low urgency/pressure
Tool tunnel vision

Cybersecurity training categories

2.2. Wargame - Defensive

	Teamwork	★		Preparation: 1-7 days
	Difficulty	★★★★		Execution: 30-120 min per target
	Setup	★★		Verify: IOC validation + time to finding
	Realism	★★		
	Ops-Pressure	★		

Cybersecurity training categories

3. Guided Labs

 Structured skill build, safely


 Read → Do step → Check → Repeat


 Step-by-step labs with checks/hints

 First-contact ambiguity and fear

 New learners • cross-trainers • onboarding

 Instant • lab grader / hints

 Clear path, low friction
Safe mistakes, quick retries
Measurable progress

 Over-guidance risk
Shallow real-world transfer
Predictable tasks

Cybersecurity training categories

3. Guided Labs



Teamwork



Difficulty



Setup



Realism



Ops-Pressure



Preparation: 1-14 days











Execution: 15-90 min per lab



Verify: lab pass + reflection + no-hints rerun

Cybersecurity training categories

4. Jeopardy CTF

- | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p> Breadth, research, fast problem-solving</p> <p> Pick → Research → Analyze → Solve → Flag</p> <p> Timed board of independent challenges</p> <p> Wide exposure; safe failure; shared learning</p> <p> Students • self-learners • teams • recruiters</p> <p> Instant • scoreboard/flags</p> | <p> High engagement, scalable
Strong write-ups culture
Great for recruiting</p> <p> Low operations realism
Puzzle drift from reality
Uneven difficulty spikes</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Cybersecurity training categories

4. Jeopardy CTF



Teamwork



Difficulty



Setup



Realism



Ops-Pressure



Preparation: 1-3 months











Execution: 5-48 hours



Verify: points + writeup + anitcheat

Cybersecurity training categories

5. King of the Hill

- | | |
|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p> Live hardening under contention</p> | |
| <p> Seize → Stabilize → Monitor → Defend</p> | <p> Real-time pressure, real fixes
Service-focused hardening
Clear, fast scoring</p> |
| <p> Shared host; hold control with uptime</p> | |
| <p> Prioritization and ownership under pressure</p> | |
| <p> Red/blue hybrids • SRE/SOC pairs • pre-A/D</p> | <p> Degenerate tactics risk
Chaotic without roles
Shallow process depth</p> |
| <p> Minutes • health checks / control score</p> | |

Cybersecurity training categories

5. King of the Hill



Teamwork



Difficulty



Setup



Realism



Ops-Pressure



Preparation: 2-4 months



Execution: 1-3 hours



Verify: Control time + uptime;
change log; eviction proofs

Cybersecurity training categories

6. Attack-Defense

a.k.a. Red Team vs. Blue Team

- ❗ Execute while under active attack
- 🔄 Detect → Patch → Attack → Automate
- ? Run services; defend uptime; exploit peers
- ⚠️ Resilience, triage, prioritization under fire
- 🧑 Red+Blue+Purple+AppSec
- 👍 Minutes • scorebot ticks (uptime + captures)
- ⊕ Uptime-first decision making
Real patch-and-protect
Offense informs defense
- ⊖ Scoring can skew behavior
Noisy “dirty” tactics risk
Host/service bias, not enterprise

Cybersecurity training categories

6. Attack-Defense



Teamwork



Difficulty



Setup



Realism



Ops-Pressure



Preparation: 3-5 months



Execution: 4-12 hours



Verify: Uptime curve + capture log +
patch diffs + incident notes

Cybersecurity training categories

7. Incident Response Drill




- ① Execute IR playbooks under time
- ↳ Alert → Investigate → Contain → Report
- ? Facilitated team drill on your tools
- ⚠ From docs to habit; smoother handoffs
- 👤 SOC, IR lead, SRE/IT, manager
- 👍 Minutes • alerts + facilitator

- ⊕ Real telemetry, real tools
Repeatable, targeted practice
Better comms and handoffs
- ⊖ Alert whack-a-mole risk
Tooling/vendor bias
Limited red creativity

Cybersecurity training categories

7. Incident Response Drill

	Teamwork	★★★★
	Difficulty	★★★
	Setup	★★
	Realism	★★★★
	Ops-Pressure	★★★★

	Preparation: 2-4 weeks
	Execution: 1-3 hours
	Verify: IR timeline
	containment evidence
	updated rule/playbook
	comms log
	time-to-detect/contain

Cybersecurity training categories

8. Purple-Team Exercise

- ① Close detection gaps fast
- 🔄 Emulate → Observe → Tune → Re-test
- ❓ Red runs TTPs; Blue tunes detections live
- ⚠️ Findings → fixes with evidence
- 👤 SOC/IR leads • Red team
- 👍 Minutes–hours • detection hits + logs
- ⊕ Evidence-driven improvement
Shared attack-defense context
Repeatable, scoped sprints
- ⊖ Demo theater risk
Scope creep/fatigue
Needs disciplined tracking

Cybersecurity training categories

8. Purple-Team Exercise



Teamwork



Difficulty



Setup



Realism



Ops-Pressure



Preparation: 1-2 months



Execution: 1-5 days



Verify: Rule/config diffs









before/after hits

ATT&CK mapping

evidence screenshots

Cybersecurity training categories

9. Tabletop

- | | |
|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p> Align roles, decisions, messaging</p> | |
| <p> Scenario → Decide → Communicate → Assign</p> | <p> Clear ownership and paths
Low cost, fast cadence
Cross-functional alignment</p> |
| <p> Prepared incident discussion → no keyboards</p> | |
| <p> Confusion on ownership and escalation</p> | <p> Talk-only risk
Vague answers without prep
No technical skill gain</p> |
| <p> Exec/Legal/PR/IT/Sec leads</p> | |
| <p> Minutes • facilitator outcomes</p> | |

Cybersecurity training categories

9. Tabletop

	Teamwork	★★★★★		Preparation: 1-3 weeks
	Difficulty	★		Execution: 1-3 hours
	Setup	★		Verify: Decision log owners/deadlines comms drafts
	Realism	★★★		
	Ops-Pressure	★★★★		

Cybersecurity training categories

10. Cyber warfare simulation

a.k.a. Cyber Defense Exercise (CDX) or Live-Fire

- ① Validate people, process, tech end-to-end
- ↳ Assign → Detect → Decide → Recover
- ? Multi-role range with live red + business injects
- ⚠ Real readiness under pressure and governance
- 👤 Whole org + partners/regulators
- 👍 Minutes–hours • composite scoring/injects
- ⊕ True resilience picture
Leadership under stress
End-to-end gaps exposed
- ⊖ Heavy prep and staffing
Safety/scope management
Hard to repeat often



Cybersecurity training categories

10. Cyber warfare simulation



Teamwork



Difficulty



Setup



Realism



Ops-Pressure



Preparation: 3–12 months



Execution: 4-12 days



Verify: After-action report (AAR)
prioritized fixes
policy/process changes

FORMAT	OUTCOME	WHEN TO USE	TEAMWORK	DIFFICULTY	SETUP	REALISM	OPS	PREP	EXECUTION	PROOF
Katas	actions become automatic	onboarding; fix slow step	1	2	1	3	2	1 day	10-20 min	filled template, trendline
Wargame (Offensive)	discovery to exploit fluency	solo, enumeration, learn exploits, tool fluency	1	4	2	2	1	1-7 days	30-120 min	flag + writeup
Wargame (Defensive)	investigate to explain fluency	solo, investigation, DFIR, evidence writing	1	4	2	2	1	1-7 days	30-120 min	IOC list + narrative
Guided Labs	safe, structured skill build	first exposure, curriculum track	2	2	2	3	2	1-14 days	15-90 min	lab pass + reflection
Jeopardy CTF	breadth & research discipline	community, recruiting, benchmark	3	4	4	3	2	1-3 months	5-48 hours	flag + writeup
King of the Hill	seize, stabilize, monitor, defend	prioritize under pressure, exploit and monitor	4	3	2	2	3	2-4 months	1-3 hours	hold time + uptime
Attack-Defense	detect, patch, attack, automate	exploit under attack, patch and automate	4	4	3	4	4	3-5 months	1-12 hours	uptime + captures + patches
IR Drill	playbook under time	playbook reps, handoffs, coach comms	4	3	2	4	4	2-4 weeks	1-3 hours	IR timeline + updated rule
Purple Team	close detection gaps fast	close gaps fast, prove detection, share context	4	3	2	4	5	1-2 months	1-5 days	before/after hits + evidence
Tabletop	decision & directions aligned	align roles, test decision, practice messaging	5	1	1	3	4	1-3 weeks	1-3 hours	decision log + owners
Live-Fire	end-to-end org validation	end-to-end, stress management, cross-stakeholder	5	5	5	5	5	3-12 months	4-12 days	AAR + fixes

Thank you

