# The Mind is the Attack Surface: A Hands-On Primer in Cognitive Security

## Summary

Cybersecurity has long focused on firewalls, patches, and scripted defenses against technical exploits. But what do we do when the target is cognition itself? How does one defend against cognitive threats?

This hands-on workshop introduces the emerging field of cognitive security and the impact it has on our industry. Through interactive exercises, participants will experience their own cognitive blind spots firsthand and quickly learn how to start defending against potential exploitation.

Join us as we map biases, introduce frameworks, run adversarial simulations where teams weaponize psychological levers against each other, and build practical toolkits for everyday defense.

Participants will leave with:

- A clear definition of cognitive security and how it differs from cybersecurity.
- Firsthand recognition of cognitive biases and vulnerabilities that can compromise even seasoned professionals.
- Practical countermeasures, open-source tools, and exercises for cultivating resilience.

Are you ready to experience a reality pentest for your brain? Come ready to challenge your assumptions, and leave with new defenses you didn't know you needed.

## Outline *(3h)*

### Module 1: Establishing a Comfort Zone *(35m)*

#### Instruction: What? How? Why?

Introduction to cognitive security vs cybersecurity.

#### Exercise: Overconfidence Honeypots

Quick challenges that play to participants' strengths while subtly exploiting hidden biases.

#### Debrief: Bias Primer

Recognition that blind spots exist even among experts.

### Module 2: Do You Trust Yourself? *(40m)*

#### Exercise: Building Cognitive Profiles

Identify personal and group vulnerabilities (biases, framing, trust heuristics).

#### Exercise: Overload & TMI

Simulation of information flood with critical ignoring techniques.

### Debrief: Exercise Insights

Intro to core frameworks and mapping biases into structured taxonomies.

## (BREAK - 10m)

## Module 3: Cognitive Security Playbook *(55m)*

### Instruction: Frameworks, Taxonomies, Research

Connecting lived exercises to formal science (DISARM, CAT, Cambridge, etc).

### Exercise: Red v Blue Simulation

Teams alternate between designing and defending against cognitive exploits (authority, social proof, urgency, etc).

### Debrief

Recognition that cognitive attacks succeed not because of weak tech, but because of human overconfidence and overload.

## Module 4: Action Planning *(40m)*

### Discussion: Actionable Insights

Risk analyses, threat mapping, and the uncomfortable statistics about cognitive vulnerabilities.

### Exercise: Build Your Own Toolkit

Explore DIY pentesting and defensive builds alongside open-source cogsec platforms.

### Debrief: Closing Reflections

Participants re-define cognitive security in their own words and make commitment to integrate resilience practices.