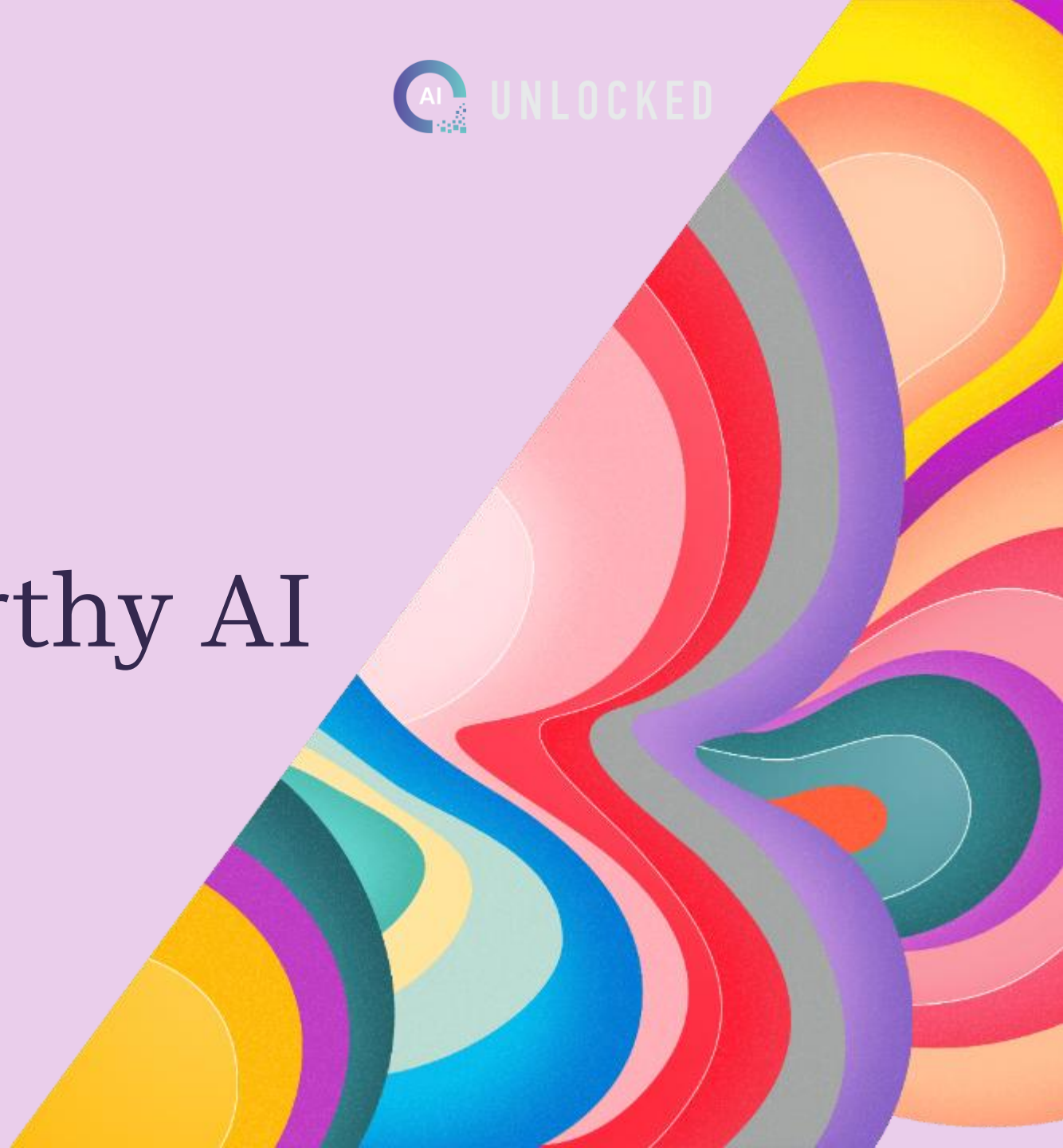
Microsoft

AI UNLOCKED

# ‘AI Unlocked’: Campus Edition Track 5 – Trustworthy AI

Build. Create. Compete.



# Track 5 – Trustworthy AI

Build a Trustworthy AI applications to improve security, and reliability of AI usages responsibly by design.

The Trustworthy AI challenge invites participants to create real-world AI security solutions that prioritize security, privacy, safety, and governance—protecting data, models, prompts, and outputs from emerging threats.

Experiment with Microsoft's comprehensive AI security ecosystem using Azure credits to implement secure-by-default architectures, identity and access controls, content safety filters, and robust monitoring capabilities. Leverage Azure OpenAI, Azure AI Services, and Microsoft Security tools to build AI solutions that organizations and users can trust at scale.

The goal is simple: ship AI that's production-ready and resilient against real-world security challenges, ensuring that innovation and trust go hand in hand.

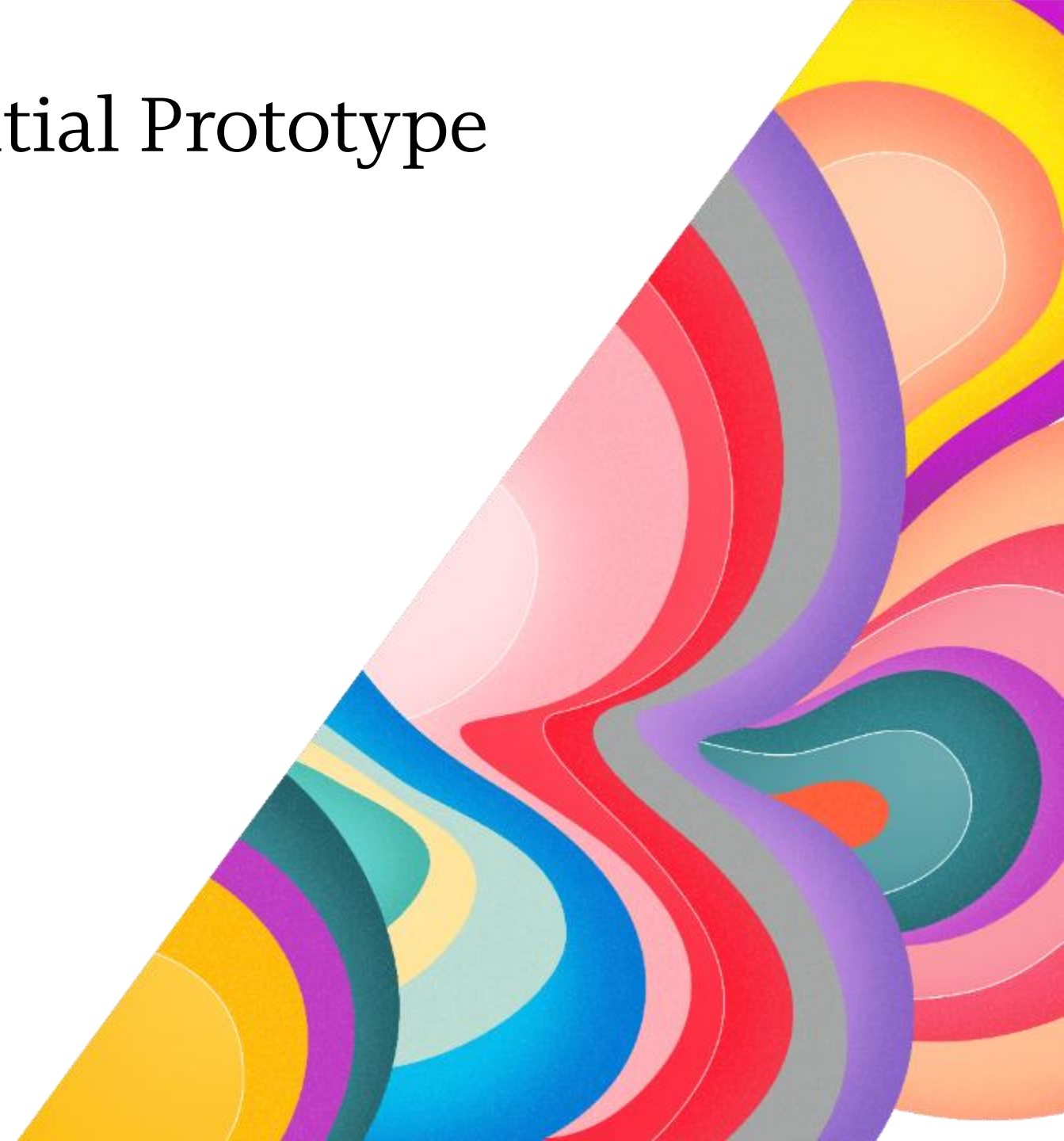
# Phase 3 Expectation : Initial Prototype

Think: **Proof of Concept in Action**

- Core functionality working
- Basic but functional UX - (if required)
- Key features implemented
- Demonstrates feasibility
- May have limitations or rough edges
- Built within tight timeline constraints

You are proving:

👉 ***"Perfection is enemy of good"***



# Phase 3 Submission Guidelines

✅ **Mandatory - Project Video**

- Show your prototype **working end-to-end**
- Demo should clearly show the **learning flow**
- Presentation Deck
  - Problem → Approach → Demo → What works today

➕ **Good to have**

- GitHub repository (For documentation and Design if it's is no-code/low-code)
- Deployed and Accessible
- Supporting artifacts / screenshots / documents

# How Your Project Is Judged

- **Security Impact & Threat Assessment**
  - Severity of AI security threat addressed
  - Quality of threat analysis and mitigation effectiveness
  - Demonstrated real-world organizational or user impact
- **Technical Feasibility & Implementation**
  - Code quality, architecture, and working demonstration
  - Completeness of documentation and production readiness
- **Innovation & Originality**
  - Novelty of approach and differentiation from existing solutions
  - Creative problem-solving in AI security context
- **Scalability Potential**
  - Ability to scale across users, environments, and workloads
  - Performance sustainability under growth conditions
- **Application Scope & Market Fit**
  - Clear target audience (consumer vs. enterprise)
  - Defined use cases and alignment with real market needs
- **Solution Complexity**
  - Depth of technical challenge addressed
  - Sophistication of algorithms, integrations, and layered defences
- **Team Readiness for Mentorship**
  - Collaboration evidence, communication clarity
  - Learning mindset and receptiveness to feedback

# Common Pitfalls

- ❌ Generic ChatGPT-style Bots and AI wrappers
- ❌ Many features, nothing fully working
- ❌ Big vision with no live demo
- ❌ Over-engineering instead of learning value
- ❌ Unclear or low-impact AI security problem definition with weak threat analysis
- ❌ Incomplete implementation
- ❌ Low innovation or heavily derivative solution with little differentiation

*A simple working prototype beats a complex incomplete one.*

# Q/A

# Thank You

For any Query on Azure credits & tech infrastructure, write to HackSupport@synergetics-india.com

For any Query on AI <Unlocked>, write to INDIAEIP@microsoft.com