



Microsoft Security at
**Microsoft
Ignite**



Technical Foundations of Secure AI Q&A

Session code: DIS667H

Intros

Who we are



Richard Diver
Sr. Manager
Story Design
Microsoft Security

Find me:
aka.ms/RichardDiver



Rod Trent
Senior Program
Manager - Cloud
Security and AI at
Microsoft

Find me:
aka.ms/RodsBlog



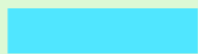
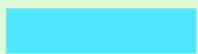
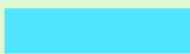
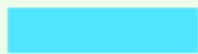
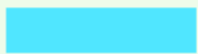
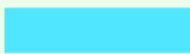
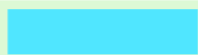
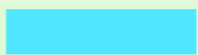









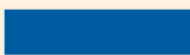






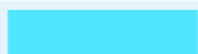

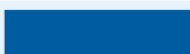
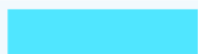

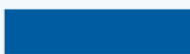
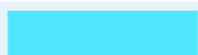




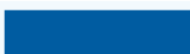
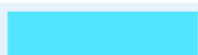





Overview





Our Discussion Today

- AI Shared Responsibility Model
- Anatomy of an AI System
- How to Assess Risks and Threats
- How to Achieve Security Success

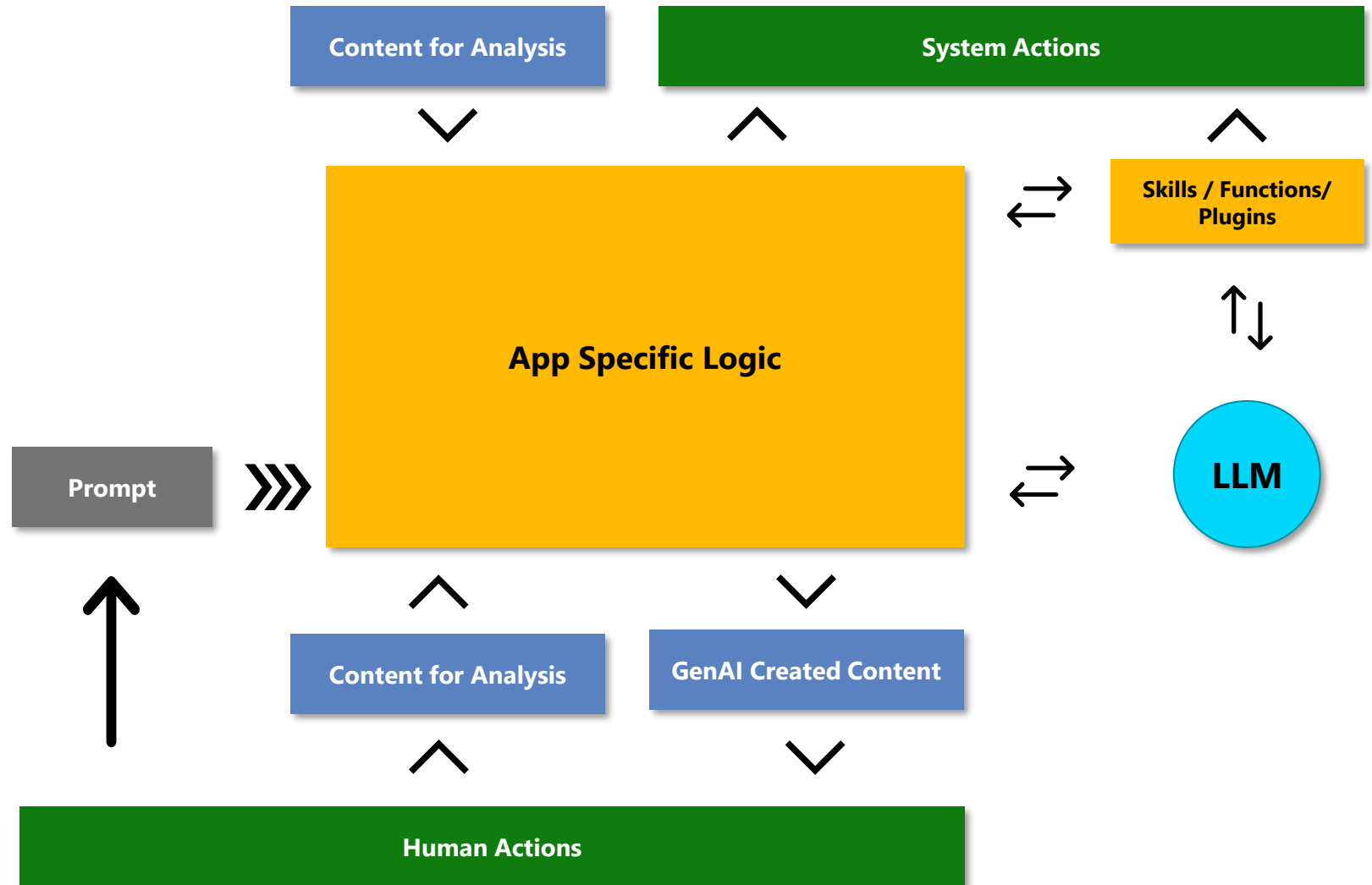
AI Shared Responsibility Model

AI shared responsibility model

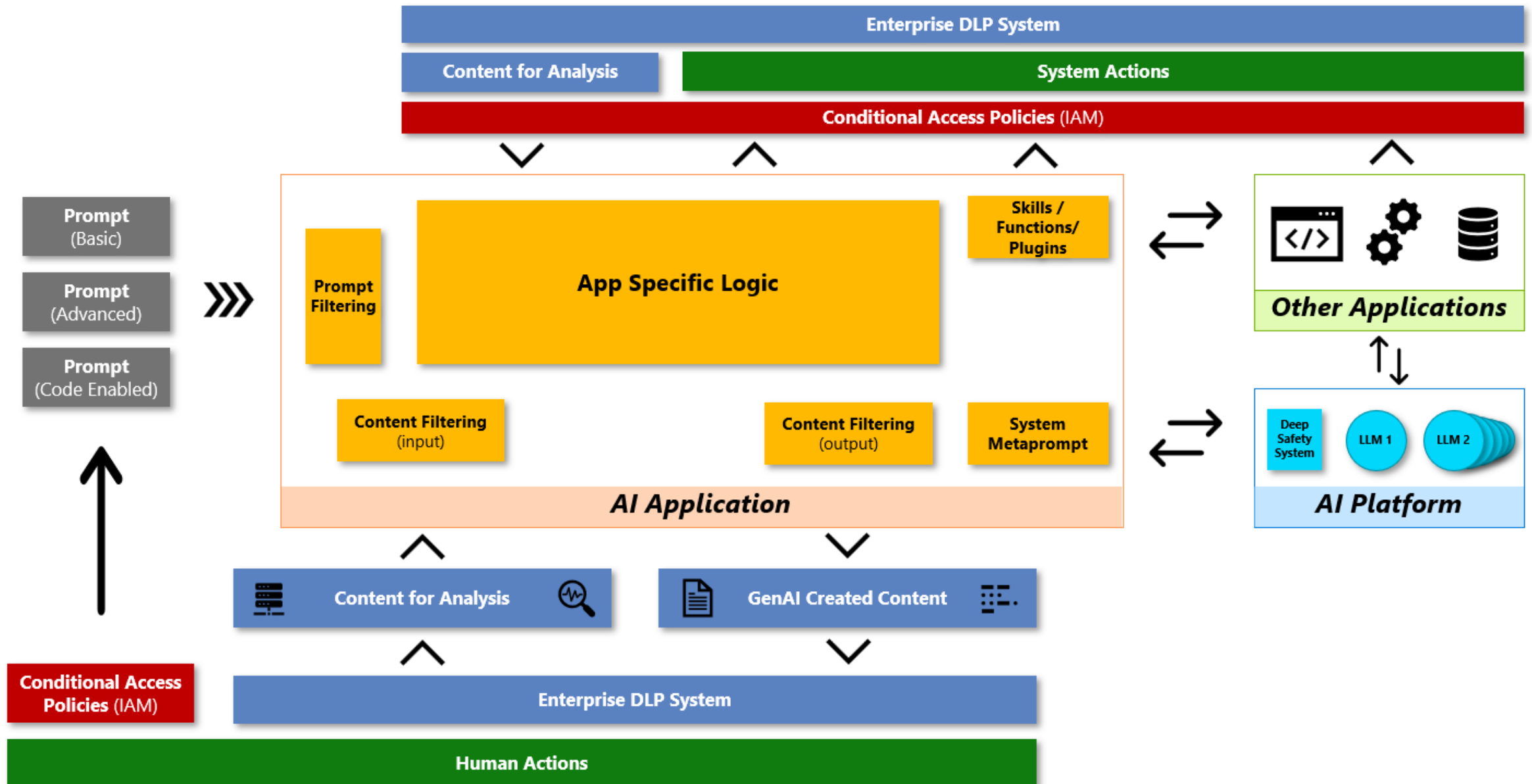
		IaaS (BYO model)	PaaS (Azure AI)	SaaS (Copilot)
AI usage	User training and accountability			
	Usage policy, admin controls			
	Identity, device, and access management			
	Data governance			
AI application	AI plugins and data connections			
	Application design and implementation			
	Application infrastructure			
	Application safety systems			
AI platform	Model safety and security systems			
	Model accountability			
	Model tuning			
	Model design and implementation			
	Model training data governance			
	AI compute infrastructure			

 Microsoft
  Model dependent
  Shared
  Customer

Anatomy of an AI System

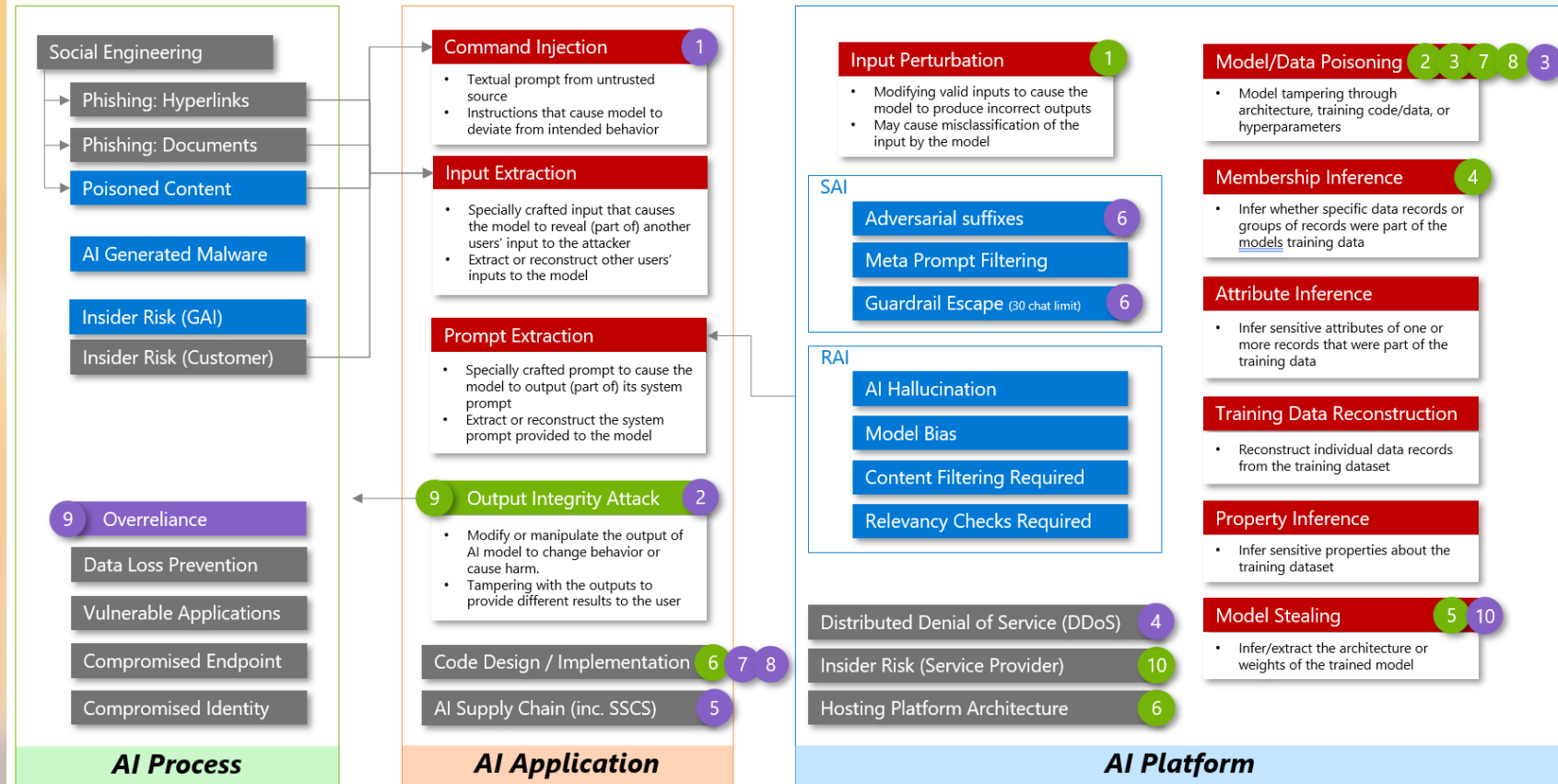


Anatomy of an AI System



Assessment: Risks and Threats

Threat Modelling Scenarios



Achievement: Security Success



- Secure Code
- Secure Data
- Secure Access
- Audit for AI threats