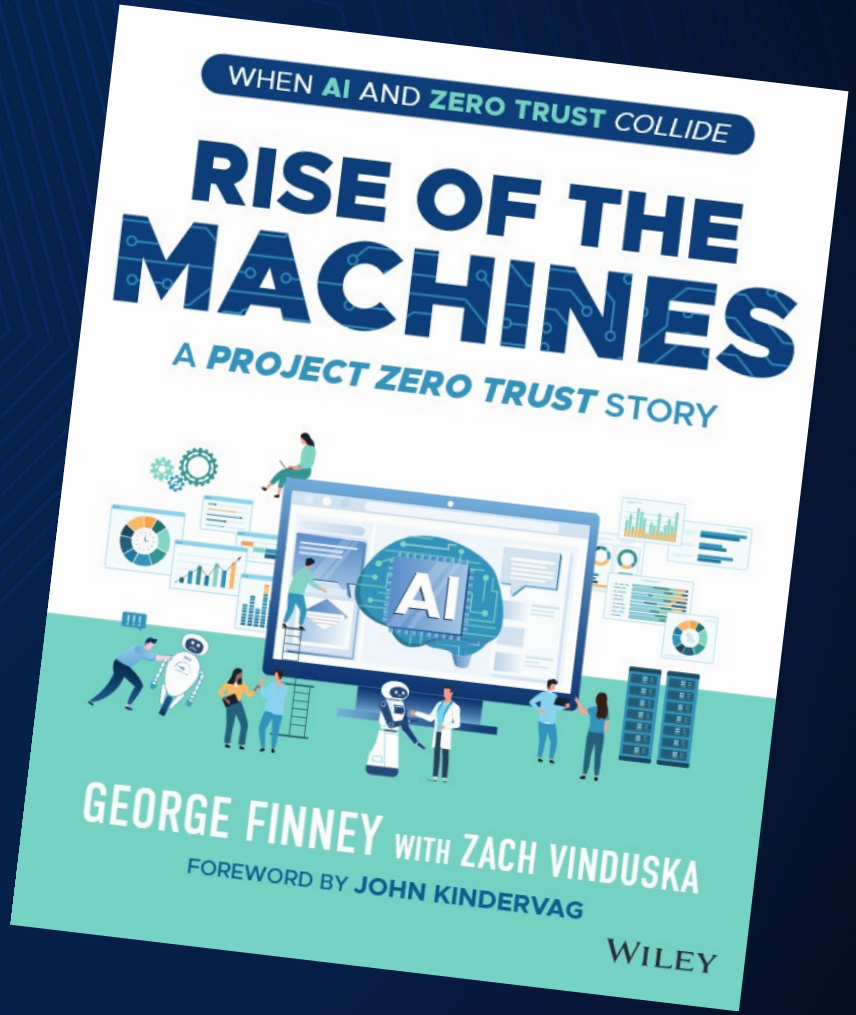
Zero Trust, Cybersecurity, and Artificial Intelligence – A Winning Team

George Finney, CISO
The University of Texas System

March 2025

The University of Texas System

Every Step Matters



The University of Texas System

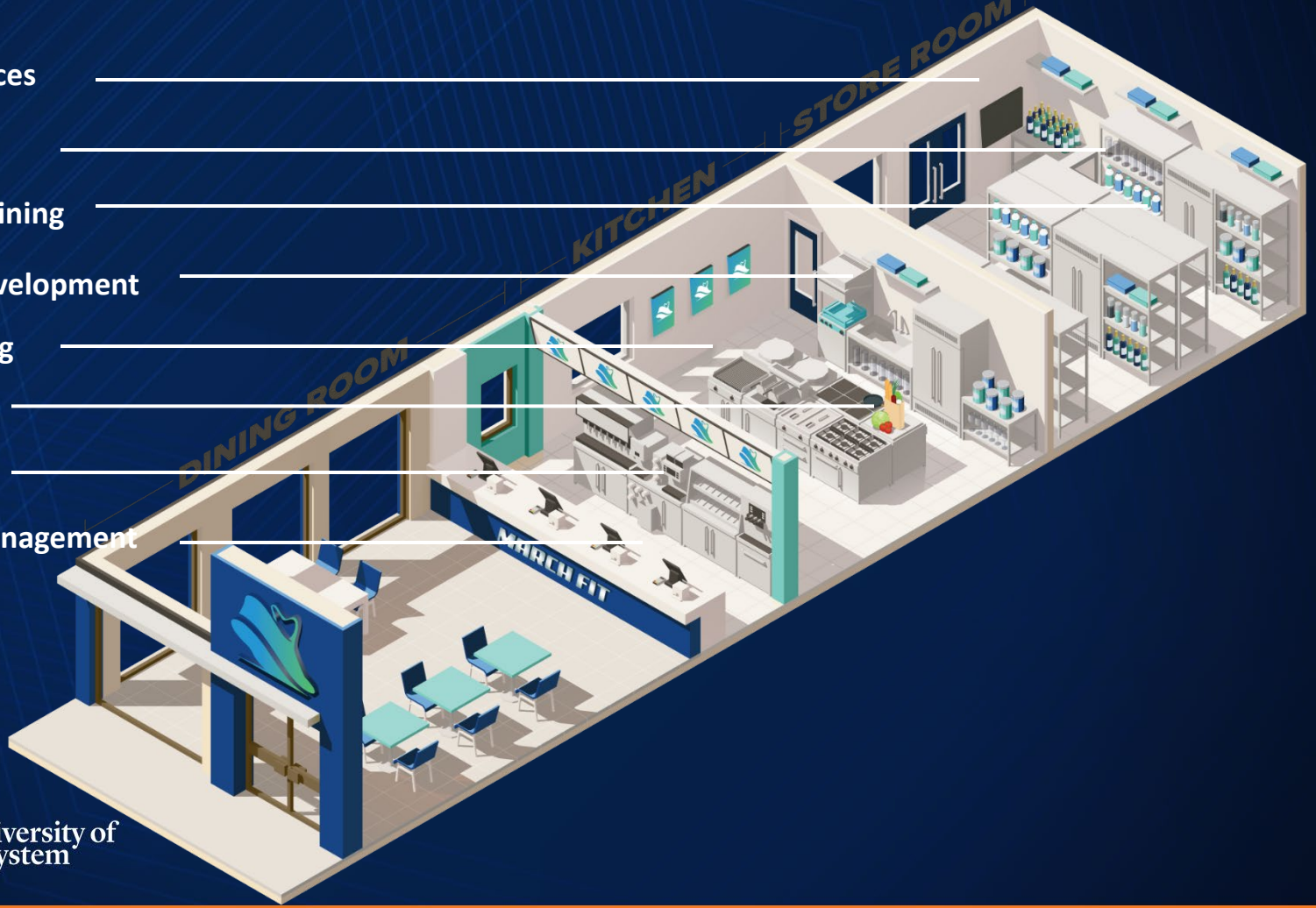
The University of Texas System

The University of Texas System

The University of Texas System

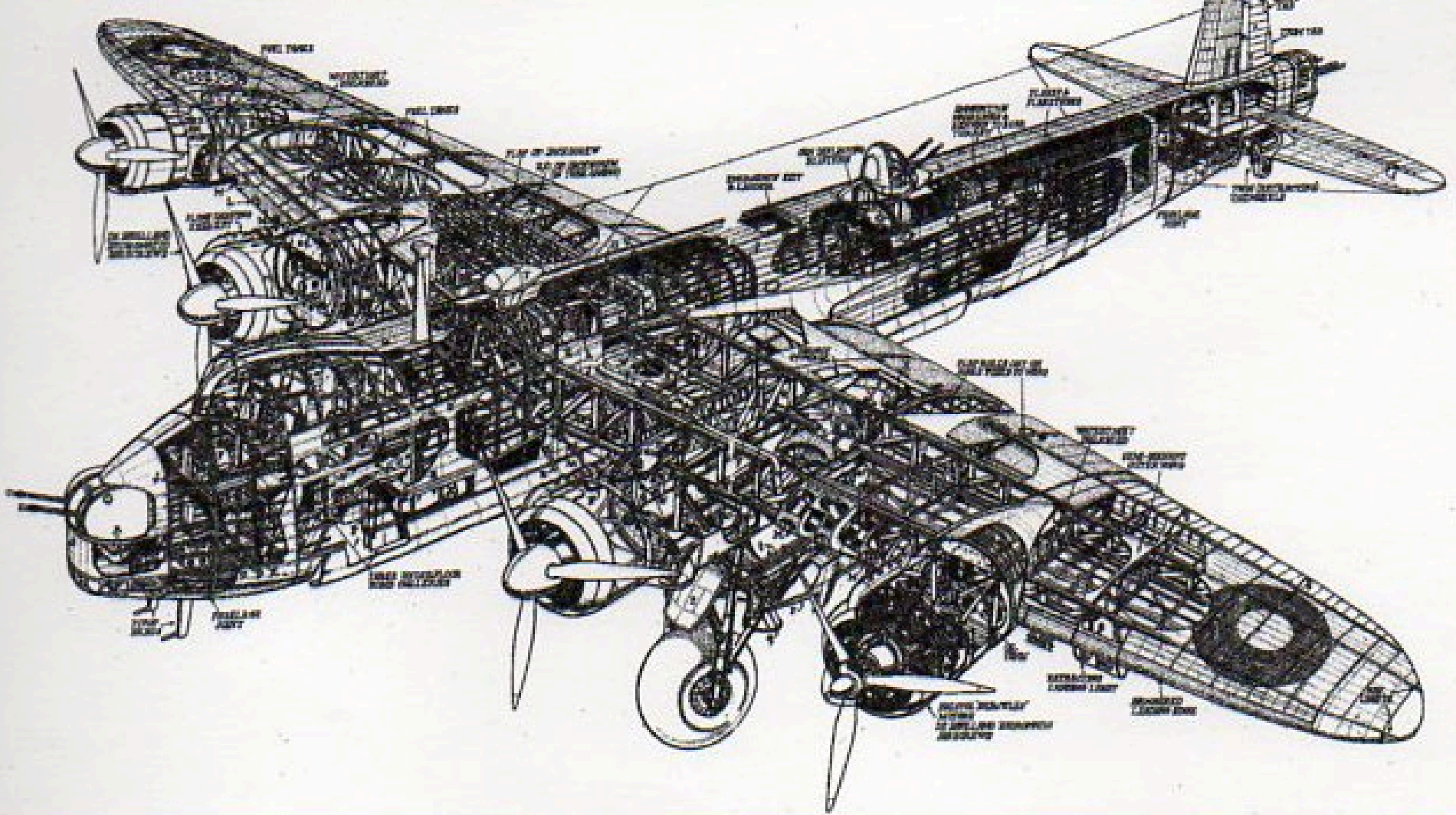
The University of Texas System

1. Data Sources
2. Data Prep
3. Model Training
4. Model Development
5. Monitoring
6. Identity
7. Serving
8. Model Management



The University of Texas System

Zero Trust | zē'rō ˈtrøst | Noun | A strategy for preventing or containing cybersecurity breaches by removing the trust relationships in digital systems.



Zero Trust Principles

1. Focus on Business Outcomes

2. Design From The Inside Out

3. Determine Who/What Needs Access

4. Inspect and Log All Traffic

Zero Trust Design Methodology

1. Define Your Protect Surface

2. Map Your Transaction Flows

3. Architect Your Environment

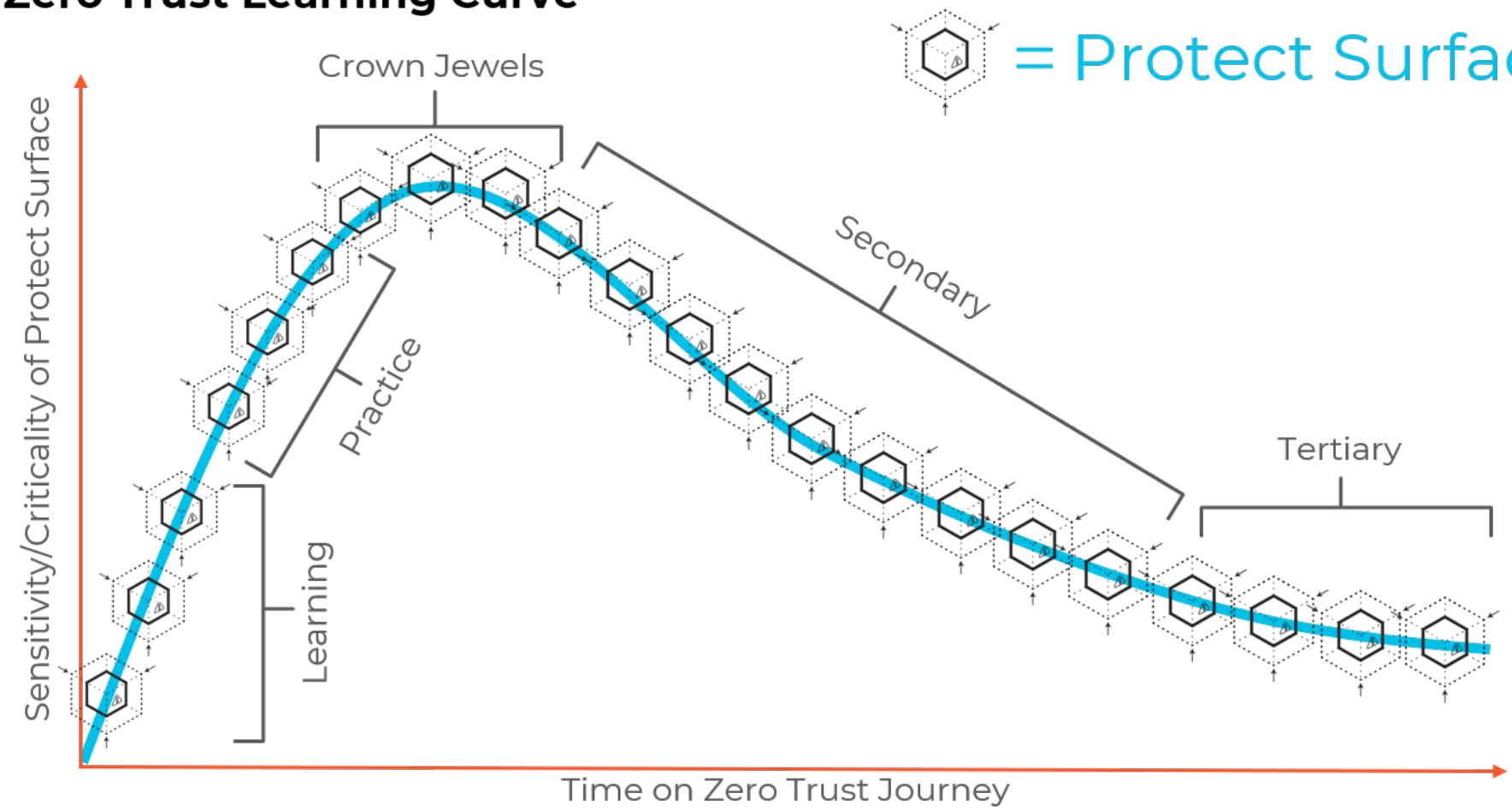
4. Create Zero Trust Policies

5. Monitor and Maintain

- Contains Blast Radius
- Auto Discovery of All Assets
- Data Classification
- Microsegmentation

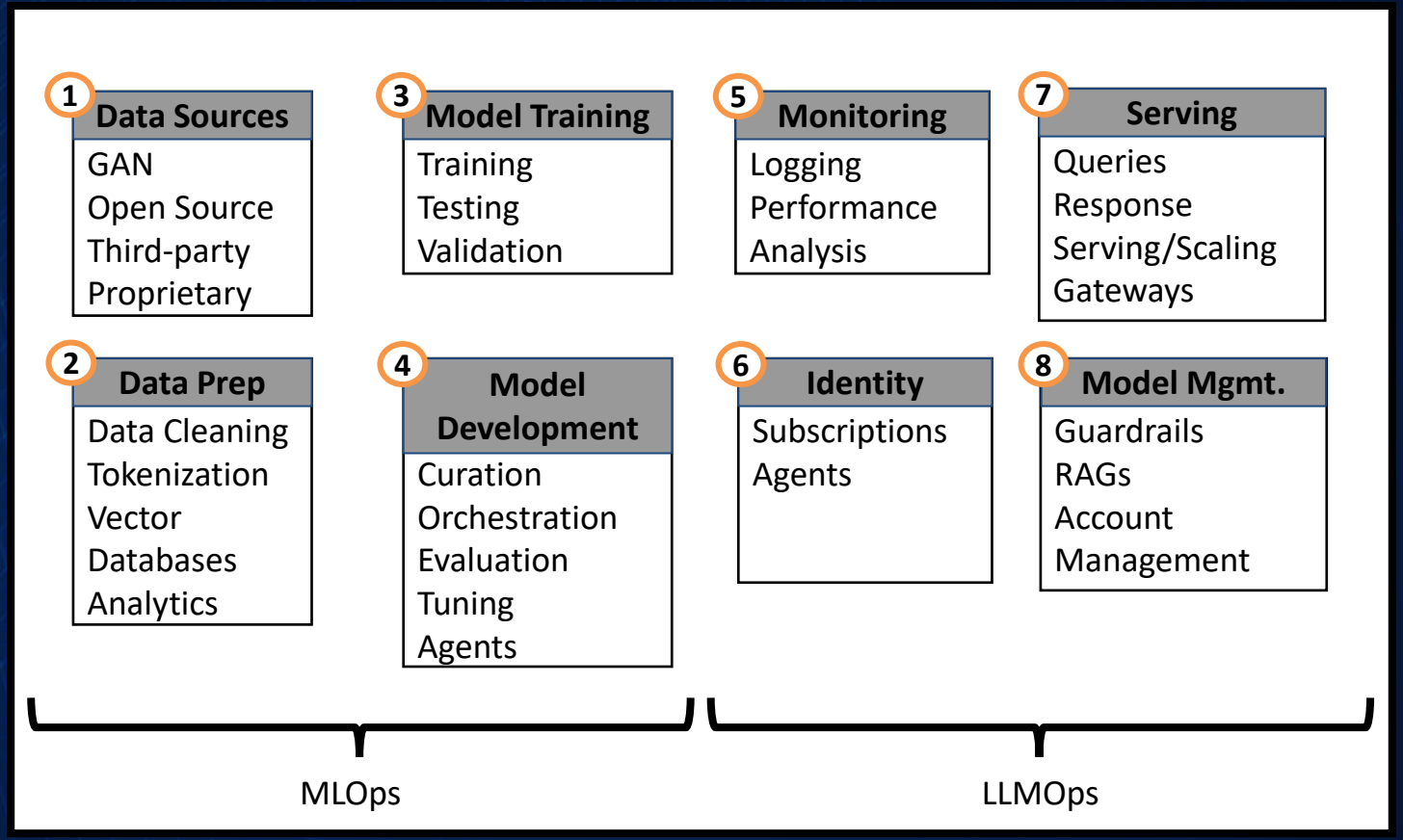
1. Define Your Protect Surface

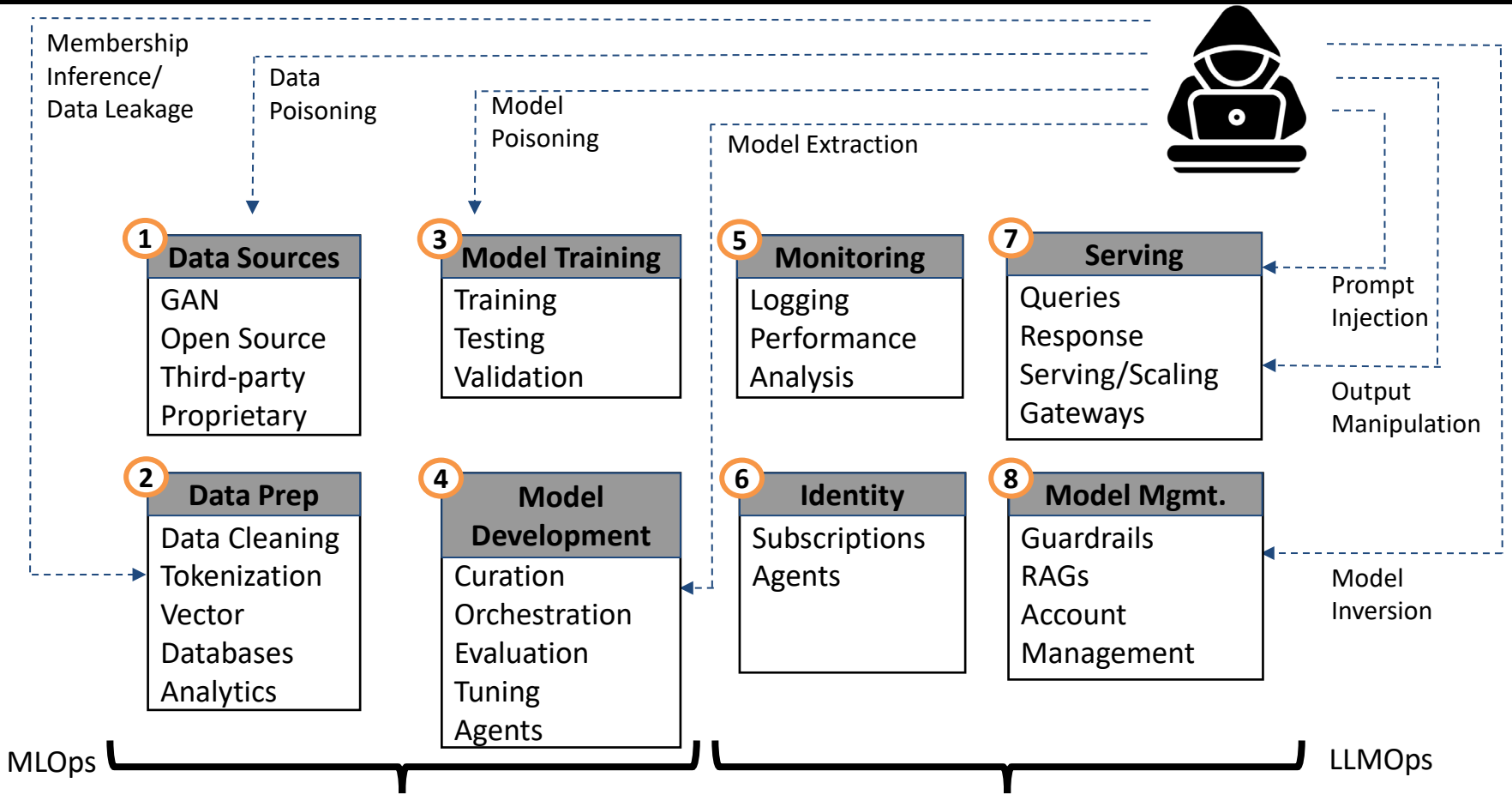
Zero Trust Learning Curve



- No Unknown Traffic
- Safelisting
- Transaction Flows are automatically mapped and visualized
- IT Governance vets all flows

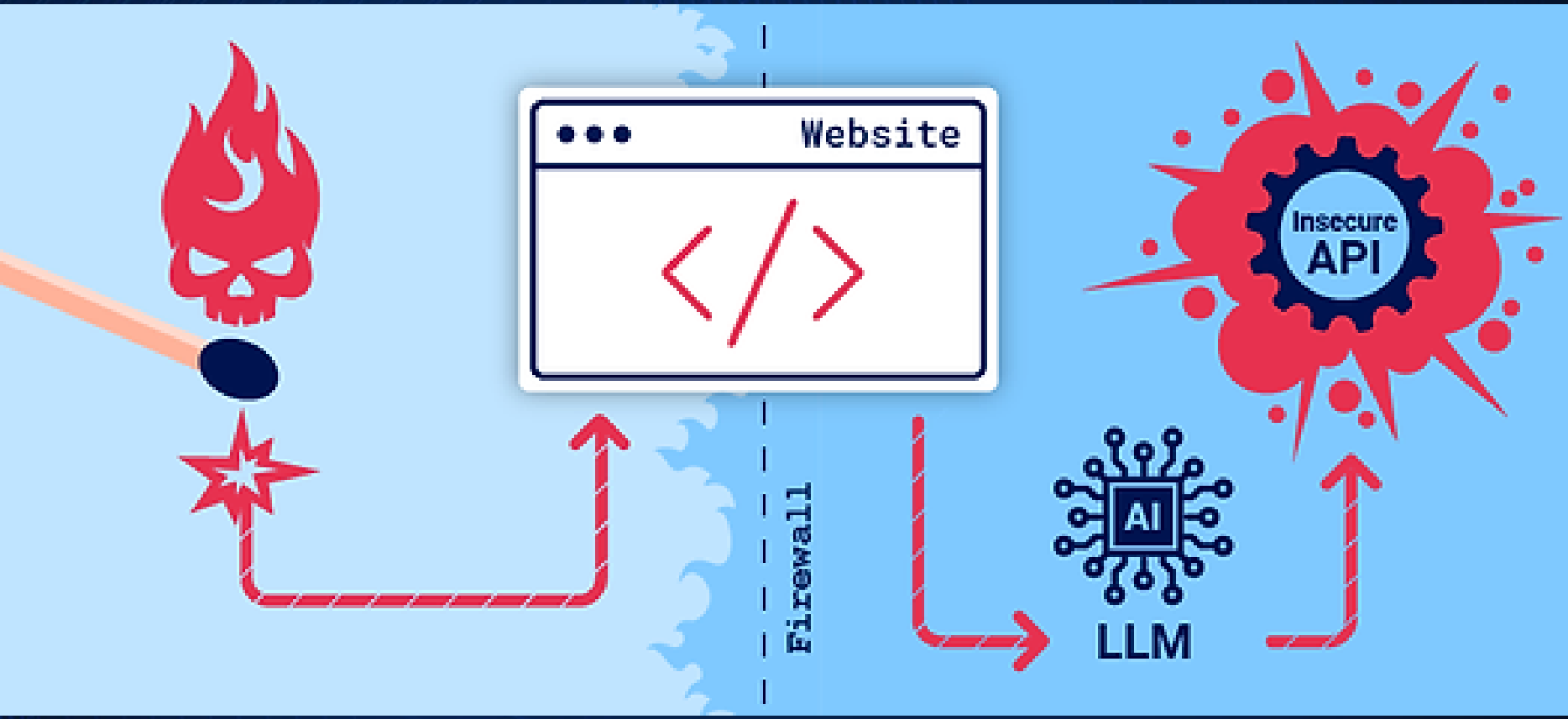
2. Map Your Transaction Flows


1
Data Sources
GAN
Open Source
Third-party
Proprietary
2
Data Prep
Data Cleaning
Tokenization
Vector
Databases
Analytics
3
Model Training
Training
Testing
Validation
4
Model Development
Curation
Orchestration
Evaluation
Tuning
Agents
5
Monitoring
Logging
Performance
Analysis
6
Identity
Subscriptions
Agents
7
Serving
Queries
Response
Serving/Scaling
Gateways
8
Model Mgmt.
Guardrails
RAGs
Account
Management
MLOps
LLMOps


Membership Inference/ Data Leakage
Data Poisoning
Model Poisoning
Model Extraction
1 Data Sources
GAN
Open Source
Third-party
Proprietary
2 Data Prep
Data Cleaning
Tokenization
Vector Databases
Analytics
3 Model Training
Training
Testing
Validation
4 Model Development
Curation
Orchestration
Evaluation
Tuning
Agents
5 Monitoring
Logging
Performance
Analysis
6 Identity
Subscriptions
Agents
7 Serving
Queries
Response
Serving/Scaling
Gateways
8 Model Mgmt.
Guardrails
RAGs
Account Management
Prompt Injection
Output Manipulation
Model Inversion
MLOps
LLMOps

3. Architect Your Environment

- No Reference Architecture
- Bespoke Controls
- Align Risk with Resources
- Red Teaming/Pre-Mortems
- Environment Specific


Website
Insecure API
Firewall
AI
LLM

4. Create Zero Trust Policies

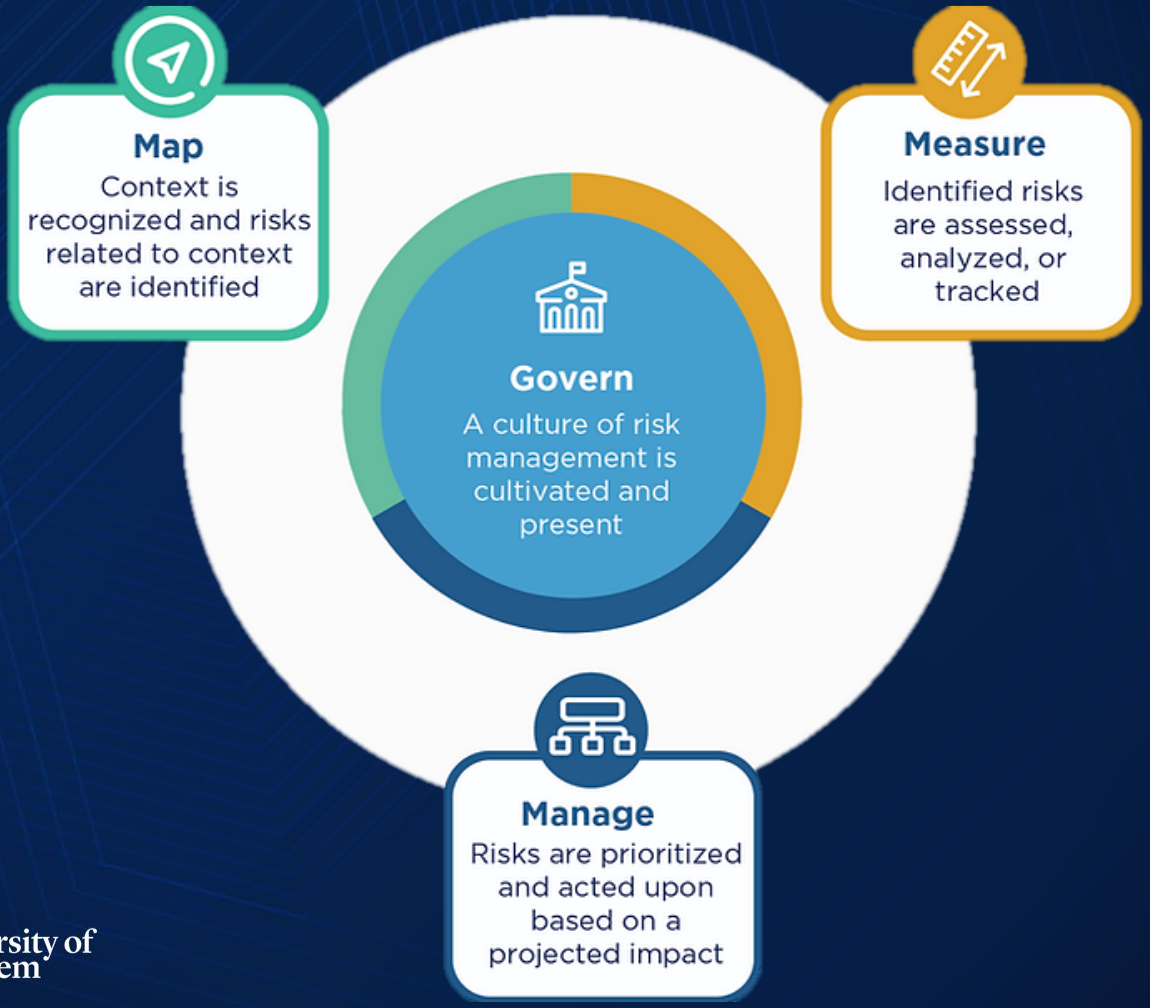
- Kipling Policies
- Layer 7 Policy
- Identity Integrations (Policy Engine, SASE, etc.)
- Terminations and Transfers
- Governance, Risk, and Compliance

Spotting The Trusts

	Identity	Device/Workload	Access	Transaction
Zero Trust for Users	Validate users with strong authentication	Verify user device integrity	Enforce least-privilege user access to data and applications	Scan all content for malicious activity and data theft
Zero Trust for Applications	Validate developers, devops, and admins with strong authentication	Verify workload integrity	Enforce least-privilege access for workloads accessing other workloads	Scan all content for malicious activity and data theft
Zero Trust for Infrastructure	Validate all users with access to the infrastructure	Identify all devices including IoT	Least-privilege access segmentation for native and third-party infrastructure	Scan all content within the infrastructure for malicious activity and data theft

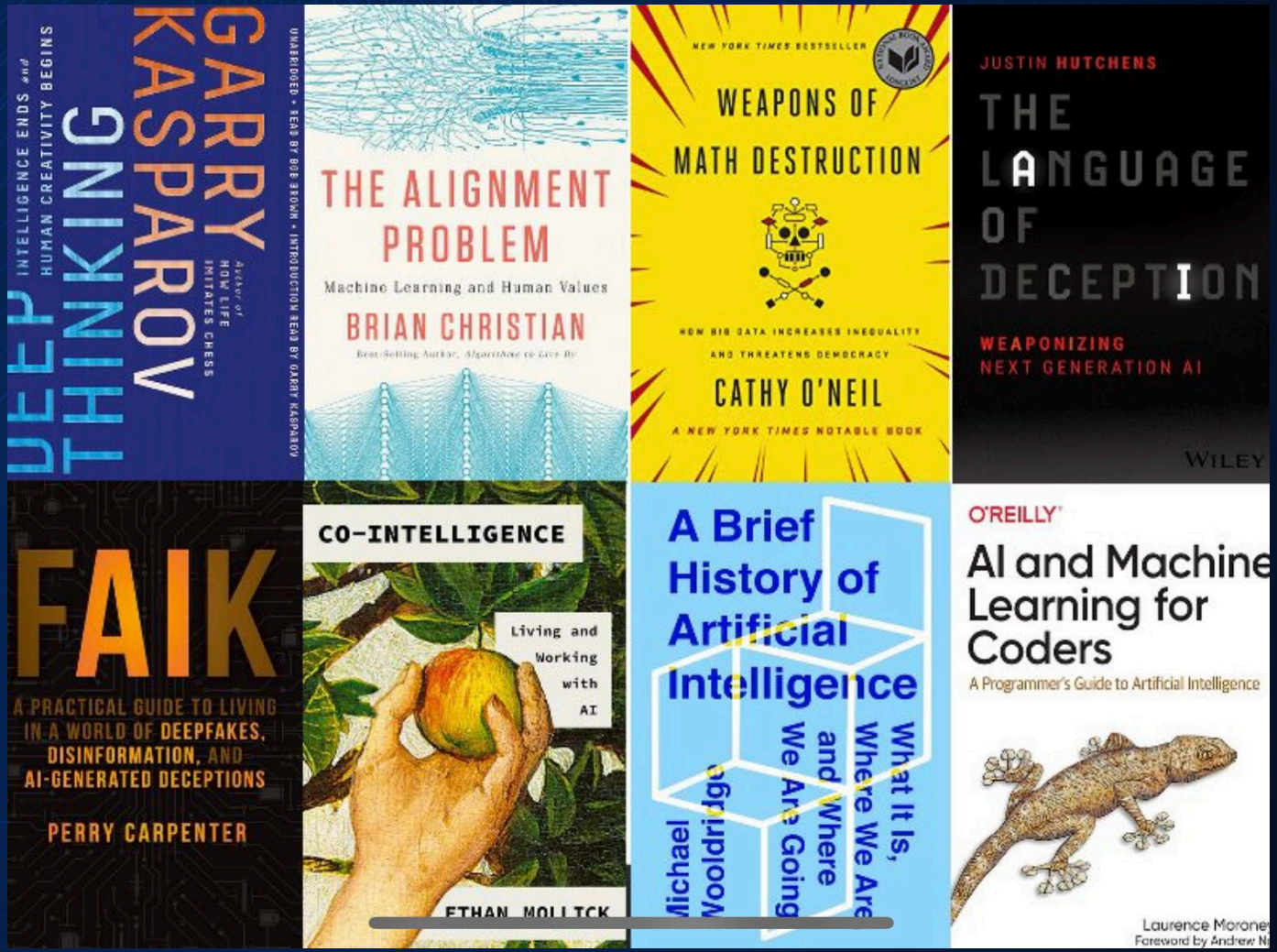
5. Monitor and Maintain

- Security Operations Center
- Managed Security Solutions Providers
- Penetration Testing
- Tabletop Exercises
- Incident Response Teams



The University of Texas System

For Further Reading



The University of Texas System

Questions?

George Finney
gfinney@utsystem.edu
linkedin.com/in/georgefinney

The University of Texas System