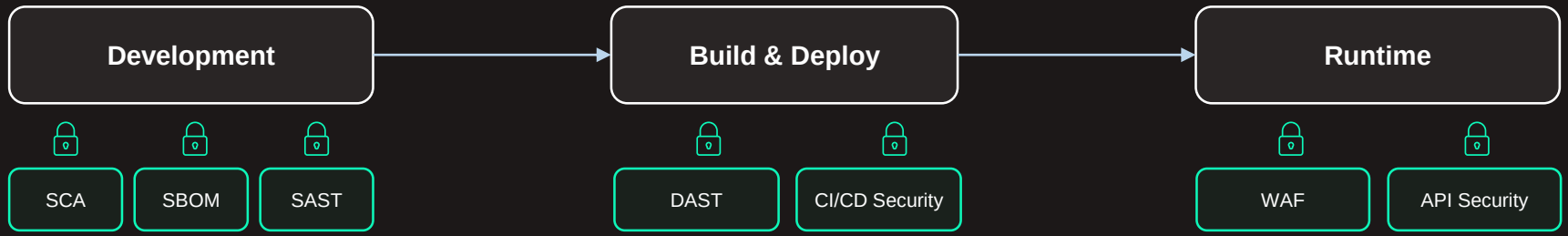
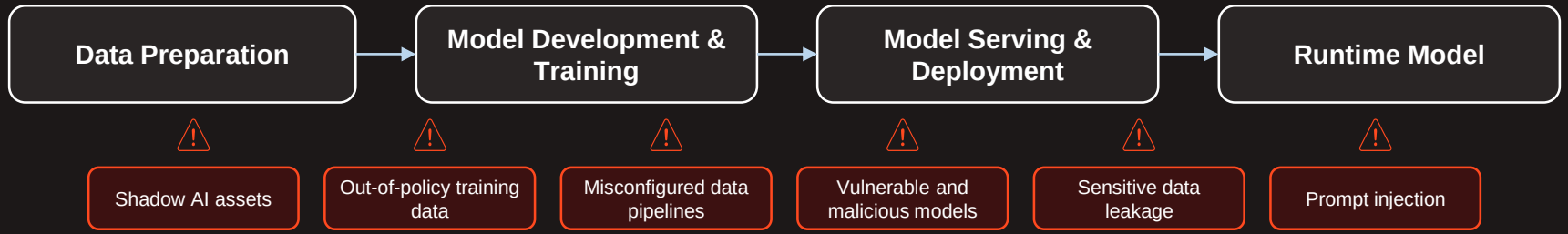
Secure Data & AI Lifecycle

	Software	Data & AI
Application	Traditional Application Security	?
Infrastructure	Cloud Security Posture Management	Data Security Posture Management

Software Lifecycle



Data & AI Lifecycle



The Data & AI Lifecycle is Unique

Unique Development Workflows

Where do the data scientists code?
Do they do it securely?

Unique Open Source Components

Are open source models and datasets malicious/vulnerable?

Unique Stack

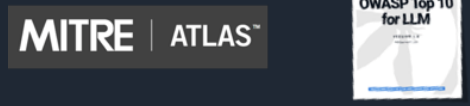
What data pipelines/MLOps tools are in use?
Are they securely configured?

Unique Data Factors

Are models trained on sensitive data or have RAG access to sensitive data?

Unique Threats

Is the application vulnerable adversarial AI attacks? Safety?

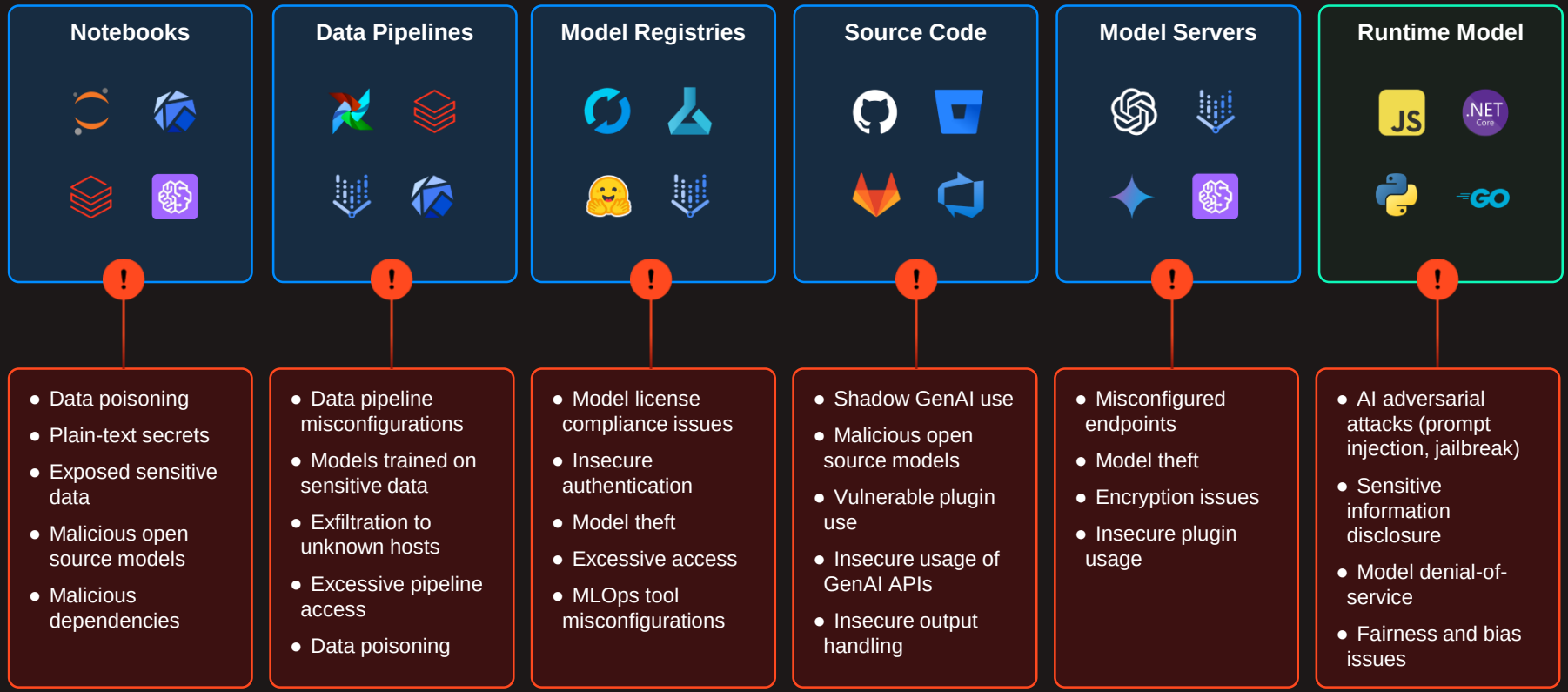


Unique Regulations

Are AI security policies and compliance regulations being met?

Risks Across the Data & AI Lifecycle

Data preparation and curation → Model development & analysis → Model serving & deployment → Machine learning operations



NOMA

Visibility, security, protection, and compliance across the entire Data & AI Lifecycle.

Data & AI Supply Chain Security

- **Jupyter Notebook Security**
- **Data Pipeline & MLOps Security**
- **Open Source AI Security**

AI Security Posture Management (AI-SPM)

- **Model Inventory and AI/ML-BOM**
- **AI Data Governance**
- **Automated AI Red Teaming**

AI Runtime Protection

- **AI Threat Detection & Response**
- **AI Safety Guardrails**

1

Simple API-Based Deployments

Deploys in minutes without any prior data science or AI expertise.

2

Coverage Across Any Environment & Stack

Supports cloud-based, SaaS, or self-hosted data & AI environments.

3

100% Frictionless for Data Science Teams

Builds a common language between data/AI and AppSec teams.

NOMA

Thank You!

Noma Security