March 2026 Cybersecurity Highlights

Major Highlight — Securing AI itself

Key developments

- **AI systems become attack targets**
  - Model poisoning
  - Data pipeline attacks
  - Prompt injection
- **Zero Trust Architecture Expands**
  - Applied to AI systems and data flows
- **Regulatory focus increases**
  - Governments pushing AI security

Path Forward

Cybersecurity is shifting from:

- Reactive defense → **Protecting AI systems themselves**