May 2026 Cybersecurity Highlights

Major Highlight — Governance-driven security

Key Developments

AI governance and security converge

- Security teams increasingly involved in AI lifecycle management
- AI risk assessments become standard practice

Model security gains prominence

- Organizations invest in protecting models from:
    - Prompt injection
    - Model theft
    - Data poisoning
    - Adversarial attacks

Identity-centric security expands

- Authentication and authorization systems evolve to support AI agents
- Verification mechanisms become critical for agent interactions

Compliance requirements increase

- New AI regulations drive investment in auditability and reporting capabilities

Path Forward

Cybersecurity is shifting from:

- "Protecting infrastructure" → **Protecting autonomous digital ecosystems**