AI Governance Sets the Rules.
AI Security Protects the System.

AI Governance

What should AI be allowed to do?

- Policies & accountability
- Risk management
- Regulatory compliance
- Responsible AI principles
- Model oversight
- Transparency & explainability
- Monitoring & accountability

AI Security

How do we protect AI from threats?

- Threat detection
- Vulnerability management
- Access controls
- Data protection
- Prompt injection defense
- Adversarial attack protection
- Incident response

www.ampcuscyber.com | letsconnect@ampcuscyber.com