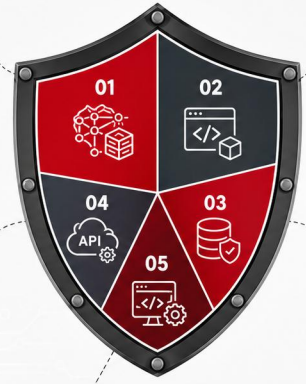
AI SUPPLY CHAIN RISKS



01 FOUNDATION MODELS

Risk: Malicious or tampered pre-trained models can contain hidden behaviors that activate under specific prompts.

Watch for:

- Unverified model sources
- Missing integrity validation
- Unexplained model behavior

02 THIRD-PARTY LIBRARIES

Risk: Open-source packages and dependencies may include vulnerable or compromised code.

Watch for:

- Outdated packages
- Dependency confusion attacks
- Unmaintained repositories

03 TRAINING DATA

Risk: Poisoned datasets can manipulate model outputs or create hidden biases.

Watch for:

- Untrusted data sources
- Lack of data validation
- Unexpected model drift

04 APIS & EXTERNAL TOOLS

Risk: AI agents often rely on external APIs and plugins that may expose sensitive data or execute malicious actions.

Watch for:

- Excessive permissions
- Weak authentication
- Unverified integrations

05 CI/CD & MODEL DEPLOYMENT

Risk: Compromised pipelines can inject malicious models, prompts, or configurations before deployment.

Watch for:

- Unsigned artifacts
- Weak access controls
- Insecure deployment workflows

www.ampcuscyber.com | Letsconnect@ampcuscyber.com