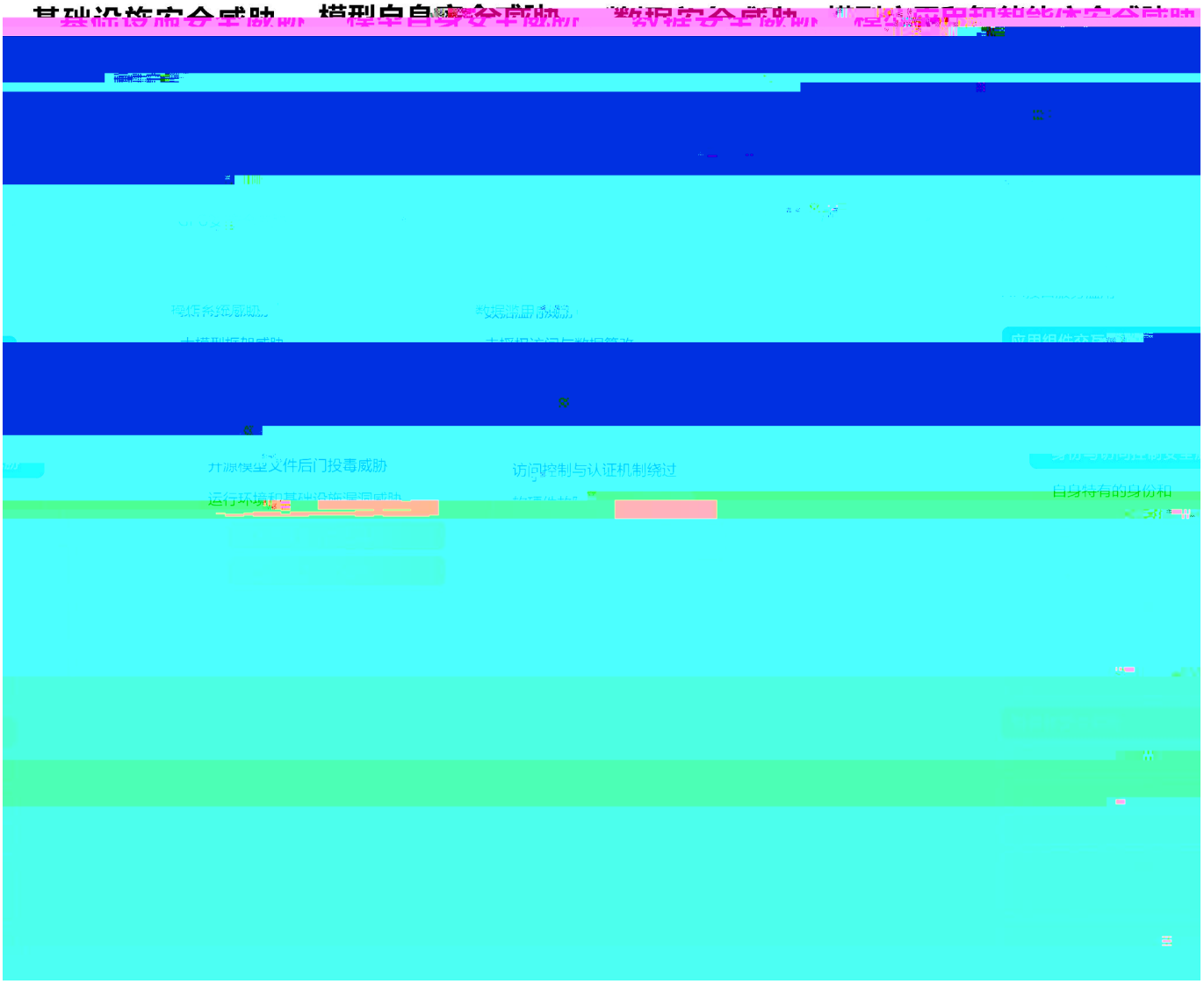
大模型安全
威胁框架

启明星辰信息技术集团股份有限公司

2025年6月


数据滥用威胁
开源模型文件后门投毒威胁
访问控制与认证机制绕过
自身特有的身份和

•

•

•

-

-

-

-

•

•

•

•

•

-

-

-

•

•

-

-

-

•