

2022新安盟年会 | 天融信 ：以“黑白融合”和安全闭环体系，应对工业变革中的行为风险

近日，2022中国网络空间新兴技术安全创新论坛年会在深圳圆满落幕。天融信科技集团深港澳大区副总经理李鑫受邀参会并发表《工业信息安全的风险与应对》主题演讲，

提出企业应构建“黑白融合”的工业行为分析体系，同时结合安全态势分析、安全防护检测、安全服务响应三维一体的安全闭环体系，实现工业信息安全体系的闭环建设。

随着工业4.0、工业互联网的推进与发展，工业进入信息化、智能化时代，云计算

、大数据等IT领域技术开始应用于工业网络。从过去的手写工单到如今的工业大数据，这是时代的变迁，也是工业领域的发展。新技术提升企业的生产效率、带来产能效益的同时，也伴随着一定的风险。

李鑫表示，基于目标环境的行为基线，天融信通过探针自下而上进行数据采集，同时结合工业信息安全态势分析系统，推出“黑白融合”的工业行为分析体系，识别工业信息安全的风险行为。同时，基于对工业信息安全体系的深入研究，天融信结合工业环境自身特点，参考国家、行业、地方安全标准，构建安全态势分析、安全防护检测、安全服务响应三维一体的安全闭环体系，实现工业信息安全体系的闭环建设。

构建“黑白融合”工业行为分析体系

工业信息安全中行为风险一般分为操作行为风险、运维行为风险和攻击行为风险，可以通过对数据变化率的技术检测、行为分析的技术手段、重要节点的报文还原分析等进行溯源，进而实现风险的识别判断。

基于对三种行为风险的识别与判定，天融信通过“黑白融合”的技术体系，识别、处置网络安全中的“灰色”行为，实现分析过程中的全面判断，实时监测工业网络的运行状态，辅以态势进行深度行为分析，由此判断访问是否存在行为风险，进而告警或防护，定位跟踪至风险源，从工业信息安全的本质解决问题。

打造运营、服务、防护的安全闭环体系

工业信息安全不仅依靠对行为分析、检测及防护，除产品和技术能力外，人的作用也至关重要，对用户的知识赋能、安全监测与保障也不容忽视。

天融信工业信息安全运营分析体系融合安全态势分析、安全防护检测、安全服务响应三大体系，依托防护检测体系作为探针采集的安全信息、以及安全服务体系提供安全数据作为分析的基础，同时对安全防护检测体系提供策略联动以及策略优化能力，安全服务体系在补充防护检测体系能力的基础前，同时对运营分析体系中安全模型、业务模型的构建与优化提供支撑。

作为最早一批开展工业信息安全领域研究和研发的企业之一，

天融信基于IPDRR工业互联网 数据安全防护模型

，可从数据的“风险识别、安全防御、安全检测、安全响应、安全恢复”五个方面，建立完善的工业互联网数据安全体系，形成数据安全建设闭环。结合工业领域数字化发展与整

体安全需求，天融信率先提出将

功能安全与信息安全充分融 合的“双安融合”理念

，将功能安全与信息安全进行有效融合，有效落实安全生产的最终目标，护航

工业互联网安全。

未来，天融信将在工业互联网安全领域继续深耕与探索，不断提升创新发展能力，持续推出创新性的产品与服务以应对新型工业互联网安全威胁，积极赋能工业互联网安全产业融合发展，为工业互联网企业网络安全保驾护航。