金钻芯 JZNM 应用安全预警系统

—产品简介—

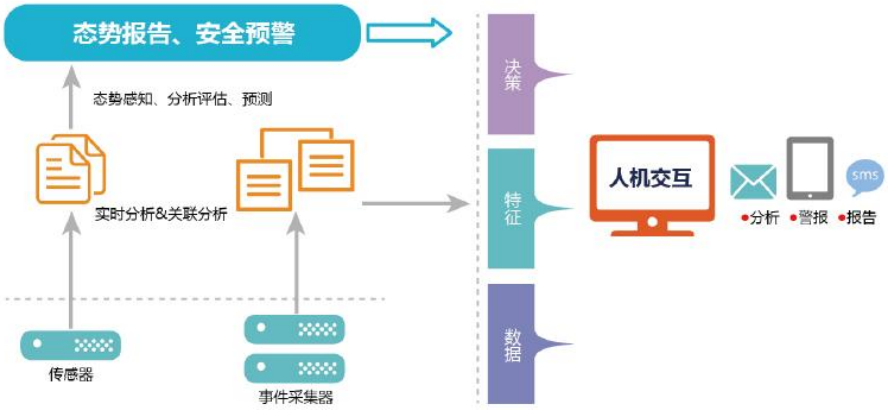
JZNM 应用安全预警系统是北京金钻芯科技有限公司结合多年在应用安全领域理论研究与应急响应实践经验积累的基础上，自主研发的一款应用级安全预警系统。基于创新的安全态势感知预警技术、精确的安全威胁与攻击识别、全面的动态的攻击行为与安全隐患分析、有机结合不同层面的安全技术与智能学习自动形成安全生态体系，通过事前预警行为预先采取相应的防御措施来提升网络与应用的安全。同时，通过有效的还原黑客攻击行为与完整的攻击事件记录，全面掌握信息安全态势，为预警、应急响应和事件调查提供支撑。广泛应用于政府、教育、卫生、电力、金融等行业，为信息安全应急保障工作提供支撑，实现信息安全事件的及时发现、定位和处置。

—产品特色—

应用安全态势感知

北京金钻芯科技在安全态势数据模型研究的基础上开展安全态势感知技术研究，解决安全态势传感器、安全态势分析与生成、安全态势的表示与可视化等关键问题。通过在网络中部署安全传感器、事件采集器，收集、监测应用的安全状态，通过采集这些传感器提供的信息，并加以分析、处理，明确所受攻击的形势，包括攻击的来源、类型、规模、速度、危害性等，明确目前应用的安全状态，

并通过可视化等手段显示给安全管理人员，从而支持安全管理人员对安全态势的了解和掌握，做出正确地响应，为应急响应提供有用情报信息。



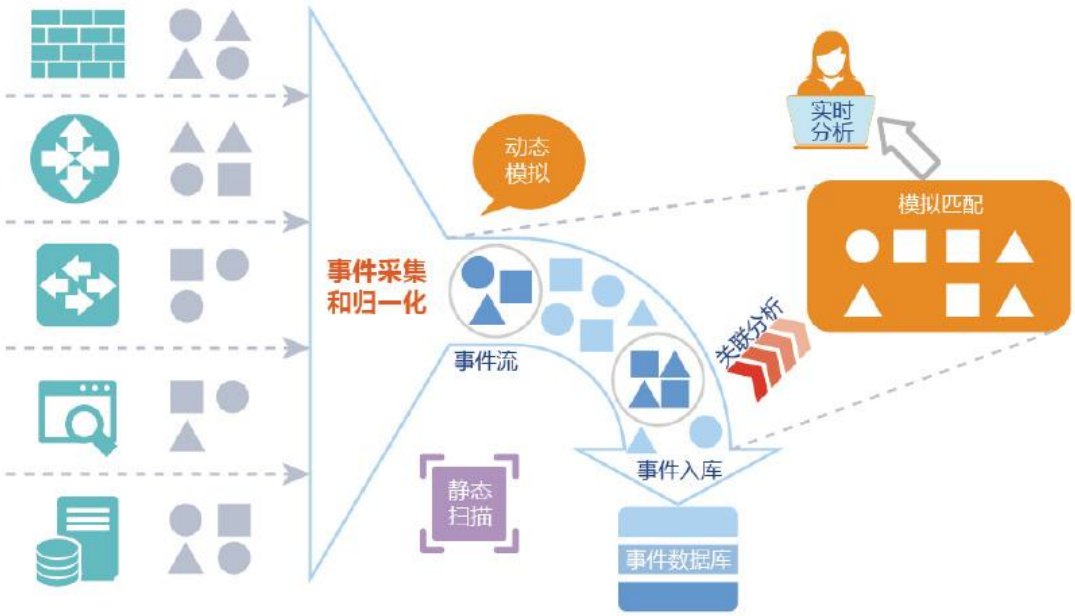
变被动为主动

面对新的安全形势，单纯的采用传统安全防护设备已经无法保证信息资产不受到新型威胁。JZNM 应用安全预警系统通过对 WEB 应用的异常跟踪，实时警报存在的威胁与脆弱环节相应的特征和特点。JZNM 应用安全预警系统对各类 WEB 攻击（已知攻击、变形攻击、未知攻击）的全方位、多层次动态的攻击提供主动的、早期的预警通报，让安全管理人员和运维人员依据风险级别及早进行防范，实现从被动的"事中"防护，走向"事前"的预警，构建一个有效的安全体系，做到防患于未然。

海量数据整合与多源告警分析

预警系统依据建立的安全态势评估指标，从不同层次、不同信息源、不同用户需求感知网络系统的安全状态，并对危险安全状态发出警报。针对不同来源的数据，基于统计、规则、状态、对象的多种方法，实现对应用安全事件的快速定

位和有效预警。通过静态扫描和动态模拟等关联分析技术，实现对应用系统安全彻底追踪与实时监测。



联动机制

Ø 应用安全联动：基于开放的联动协议，通过联动接口可以与六壬网安的安全产品联动，也支持其他安全厂商的安全产品接入。

Ø 应用预警策略联动：可与网络与信息安全应急处置平台中心实现应用预警策略库、安全应急处置预案库联动。

—典型应用—

JZNM 应用设备以旁路的方式接入到服务器交换机，通过配置服务器交换机监听口对业务应用系统安全事件进行监测，实时预警应用系统遭受到的攻击类型、数量和来源，为用户掌握应用安全状况制定信息安全政策提供基础数据和决策依据。