卫健委区域安全运营中心解决方案

1 需求背景

近年来卫生行业的信息系统数据出现多次发生信息泄露事件，人民群众的健康隐私信息的保障遭受到了极大的威胁。根据《关于落实卫生健康行业网络信息与数据安全责任的通知》要求，“各级卫生健康行政部门党委（党组）主要负责人是本行政区域内卫生健康行业网络信息与数据安全第一责任人”。

2022 年国家卫健委联合三部门发布《关于印发医疗卫生机构网络安全管理办法的通知》，其中明确坚持“管业务就要管安全”，要求各级卫生健康行政部门应建立网络安全事件通报工作机制，及时通报网络安全事件。

卫健委本级业务平台安全保障

区域卫生信息平台涉及辖区所有医疗卫生机构的数据采集和信息交互，避免出现医院间以及医院与卫健委之间的网络安全出现交叉感染。

摸清辖区内医疗机构的网络安全状况

在主管单位安全专员缺乏、安全工作统筹落地难的情况下，希望摸清辖区内医疗卫生机构网络安全现状、问题，做好汇报有数据、应急有响应、处置有建议。

重点保障区域医疗安全

如何做好辖区内医疗机构的主动防御，减少安全事件和安全部门通报发生，特别在疫情期间和重点时期更需要全面保障。

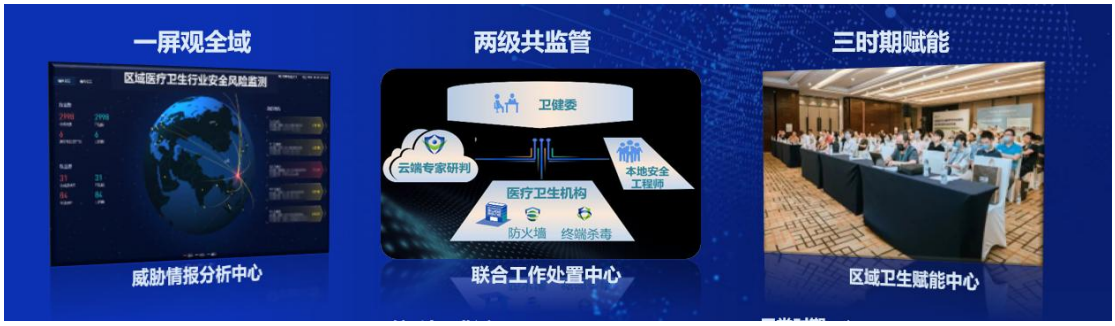
深化全员网络安全建设意识

网络安全不只是卫健委信息部门的责任，也不只是医院信息部门的责任，如何让全员参与到网络安全意识建设，更好地承接信息化建设任务，成为数字化转

型中尤为重要的一环。

2 深信服解决方案

2.1 解决思路

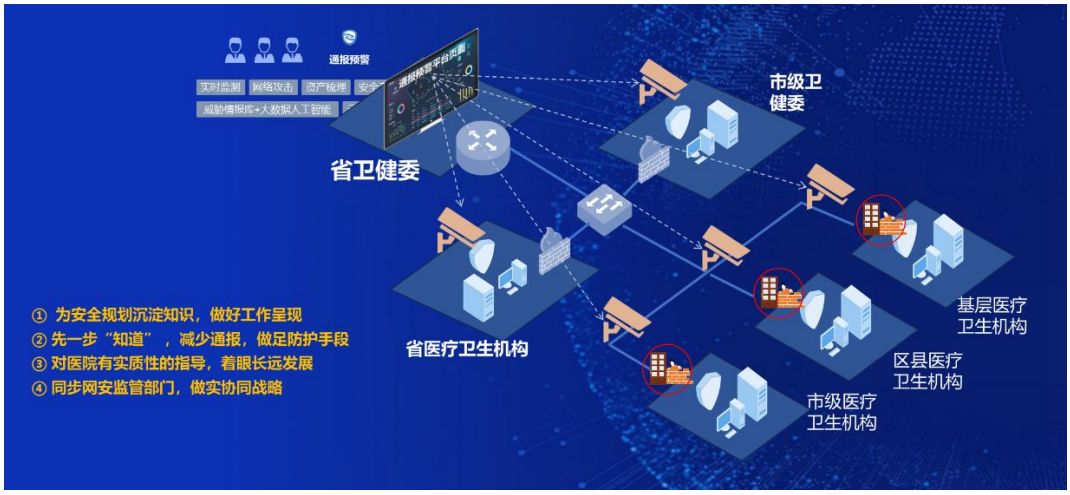


一屏观全域：让安全工作看得见。全面摸清区域医疗卫生系统重要网络及数据的安全防护现状。网络安全风险防患于未然，单个机构出现问题时能及时止损和应急。

两级共监管：卫健委重在“监测”：主要监测全市医疗网络安全情况，发现后提出整改通知，并给出指导建议（为区域整体“体检”与“体检报告”）；医院重在“管办”：本单位直接监测管理和建设，做好本院网络安全的整改和加固。通过双重监测保障，减少安全事故发生。

三时期赋能：让全员参与网络安全意识和能力建设。（1）日常时期：安全培训、技术沙龙、专业培训；（2）重点时期：政策解读与宣贯、联合检查；（3）特殊时期：攻防演练、安全规划支撑。

2.2 解决方案



- 搭建区域医疗卫生网络安全监测预警平台

借助态势感知平台/最新的 XDR（可扩展的检测与响应）安全技术搭建省卫健委本级网络安全预警平台，并通过安全日志采集设备接入下属医疗卫生机构，构建区域级的高精准检测能力、通报预警能力、应急处置能力，通过大屏轮播、实时告警等方式实现对接入单位的 7*24 小时可视化、动态化监测

- 构建“云地一体化”安全防护服务体系

由省卫健委牵头，通过联合本地专业网络安全企业，构建本地安全联合作战中心，并结合云端安全运营中心，提供区域医疗卫生机构网络安全风险溯源、处置的安全运营服务。本地安全联合作战中心重点保障本地安全风险管控能力实现 5*8 小时分钟级响应，云端安全运营中心以持续在线守护为主线，实现 7*24 小时人机共智的安全托管服务（MSS)，共同提升组织安全风险管控能力和安全工作效果。

- 健全区域医疗网络安全运营流程和制度

建立符合我省卫生行业自身情况的安全运营制度和流程，包括委本级、卫健委对医疗机构等日常告警响应、安全事故应急、安全威胁预警、资产管理等流程，并将这些线下的运营流程通过平台实现电子化的线上标准化流程。通过运营流程搭配运营团队实现实时监测系统运行状况，每周出具安全形势报告，提高安全应对能力，系统健康程度，降低安全风险。针对下属各单位制定应急响应预案，依托监管预警平台发现安全风险并给出处置方案和建议，必要时安排安全服务中心技术专家远程或上门协助相关单位进行处置，避免下属单位因技术能力不足导致网络安全风险继续扩散。

- 构建以 GPT 为核心的智能监测运营能力

为解决委本级安全人员不足的问题，采用安全垂直领域专用大模型安全 GPT 辅助安全人员进行运维工作。通过大模型智能化、自动化方式，对威胁进行自主研判、定性，权限内闭环处置，大幅度优化平均威胁检测时间和平均威胁响应时间，提升组织的安全能力，将日常安全运营所花费的时间减少 90%。

3 方案优势

- 全网业务资产监测与安全态势可视化

通过对全网业务资产进行有效识别，持续检测其脆弱性，从而及时发现业务上线及系统更新所产生的漏洞及其他安全隐患。此外，平台可以将检测到的风险以全局视角进行清晰的可视化呈现，漏洞、病毒、弱密码等全网安全风险一览无遗，为快速有效的安全处置奠定了良好基础。

- 分支机构安全态势可感知、可监管

平台支持以独立的分支为安全管理视角，展示每个分支机构/被监管机构的安全态势，分支机构管理员可单独查看所在分支的所有安全问题详情，并进行针对性的处置，不受其他分支干扰。

- 7*24 小时安全服务保障

结合深信服安全托管服务 MSS,东莞市卫生健康局采用了“人机共智”的方式建立了持续运营流程和机制，实现了 7*24 小时的持续监测和安全问题的主动响应。通过持续监测、动态发现、及时通报、协同处置等，实现全网安全风险可控和闭环处置。

4 典型案例

东莞市卫生健康局、惠州市卫生健康局、合肥市卫生健康委、潍坊市卫生健康委、烟台市卫生健康委、淮安市卫生健康委、杭州市卫生健康委、台州市卫生健康委、镇江市卫生健康委….