商业轻骑兵解决方案

政府安全监管平台解决方案

开局指导

新华三技术有限公司

http://www.h3c.com

目录

官网介绍

https://www.h3c.com/business/zf10.htm

参考设备配置清单

政府安全监管平台解决方案：

方案名称	类型	产品名称	组网应用定位	产品选型建议	备注
政府监管平台解决方案	设备	网站监测探针	互联网业务区	H3C SecCenter CSAP网站态势感知产品	监测各委办局网站风险。
		漏洞扫描设备	互联网业务区	H3C SecPath SysScan系列产品	扫描各委办局暴露在互联网上的资产漏洞信息。
			电子政务外网	H3C SecPath SysScan系列产品	扫描部署在政务云上资产漏洞信息。
		流量探针	旁挂各委办局互联网出口	H3C SecCenter CSAP-NTA，具备1.8G/2.5G/4G/6G/8G/12G，6种款型	监测各委办局互联网出口流量。
			旁挂电子政务外网骨干网核心交换机	H3C SecCenter CSAP-NTA，具备1.8G/2.5G/4G/6G/8G/12G，6种款型	监测通过政务外网骨干网的流量。
			旁挂政务云出口核心交换机	H3C SecCenter CSAP-NTA，具备1.8G/2.5G/4G/6G/8G/12G，6种款型	监测访问政务云内业务系统的流量。
	相关软件产品	网络空间资产探测探针	互联网业务区	纯软件交付，服务器单独配置	支持1万、10万、50万IP探测，用来探测各委办局暴露在互联网上的资产。
		监管类态势感知各组件授权函	互联网业务区+电子政务外网管理区	基础数据平台组件授权函/业务安全运营软件授权函/融合联动共享软件授权函/综合态势展示软件授权函/网络异常行为分析软件授权函/资产发现管理软件授权函/实时威胁监测软件授权函/网站安全监测授权函/应急响应处置软件授权函/通报预警响应软件授权函/重保指挥调度软件授权函，各组件可独立交付部署。	应急响应处置软件授权函/通报预警响应软件授权函/重保指挥调度软件授权函，此三类组件部署在互联网业务区，其他组件部署在电子政务外网管理区。

参考关键技术

方案名称	关键技术点	作用	涉及产品
政府监管平台解决方案	基础数据采集	为了满足平台分析对数据质量的要求，同时建设数据处理模块，对采集到的外部异构数据进行格式解析、校验、标准化、关联补齐和统一存储，使其从外部数据转化成内部数据，便于应用层使用。	基础数据平台组件授权函
	业务安全运营	帮助上级监控部门了解各单位网络安全现状，为网信办进行统一指挥提供基础数据支撑，同时通过网信办和各单位的联动，实现以网络安全态势感知为基础推动网络安全工作的有效落地。	业务安全运营软件授权函
	融合联动共享	融合联动共享平台主要实现多源情报采集和自主上传、情报联动交换、情报共享推送等核心功能，包括多源情报聚合、多向情报分发、情报集成订阅等在内的多项应用能力。	融合联动共享软件授权函
	综合态势展示	提供整体威胁态势、外网攻击态势、资产态势、脆弱性态势等可视化呈现能力，帮助监管单位从宏观把控区域安全态势，加强统一指挥能力。	综合态势展示软件授权函
	网络异常行为分析	基于海量的数据，对资产进行分析，建模和学习，通过已经构建的规则模型、统计模型、机器学习模型和无监督的聚类分析，构建出资产在不同场景中的正常状态并形成基线，从而有效识别行为偏移，及时发现资产存在的可疑流量行为。	网络异常行为分析软件授权函
	资产发现管理	对接网络空间资产探针探测的互联网资产数据，对接被监管单位上报的以及流量被动发现的资产数据，对属地网络资产进行全生命周期管理。	资产发现管理软件授权函
	实时威胁监测	以安全大数据为基础，从不同视角和维度进行风险呈现，实现安全事件实时监控与预警，发现潜在的安全问题，基于机器学习和专家系统，对大范围样本数据进行安全分析，发现威胁并预判趋势。	实时威胁监测软件授权函
	网站安全监测	通过爬虫技术、沙箱技术、漏洞扫描等技术以云SaaS形态为客户提供主动的网站安全监控与检测，能够主动监控网站安全问题，监测网站脆弱性。	网站安全监测授权函
	应急响应处置	当发生紧急安全事件的时候，可通过平台协同其他同级单位进行安全事件处置，通过建设事件处置基础资源库，通过平台向其他相关单位发送协同处置指令，利用基础资源开展攻击溯源、取证分析等工作，结合各方力量实现安全事件的协同处置，同时实现安全事件数据共享。	应急响应处置软件授权函
	通报预警响应	协助监管单位对安全事件进行通报、反馈、处置，实现对业务安全的全闭环，支持被监管单位信息报送，帮助监管单位掌握信息安全状况，对通报事件进行全流程记录、跟踪，做到事后统计、复盘。	通报预警响应软件授权函
	重保指挥调度	在重要会议或重大活动期间，加强网络安保人员调度，全方位全天候掌握全市与活动相关的单位、系统和网站安全状况，及时通报预警网络安全隐患，高效处置网络安全案事件。	重保指挥调度软件授权函

开局相关资料

1. H3C SecPath SysScan-AK 系列漏洞扫描系统安装指导、配置指导、典型配置举例等资料，参考以下链接

   http://www.h3c.com/cn/Service/Document_Software/Document_Center/IP_Security/LDSMXT/H3C_SecPath_SysScan-AK/?CHID=353106&v=612

2. H3C SecCenter CSAP-NTA-C[S][A]系列 流量探针安装指导、配置指导、典型配置举例等资料，参考以下链接

http://www.h3c.com/cn/Service/Document_Software/Document_Center/IP_Security/SecCenter/H3C_CSAP-NTA/?CHID=365590&v=612

3. H3C SecCenter CSAP 产品 快速安装指南-APW100 参考以下链接

   https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Security/00-Public/Quick_Starts/Quick_Installation/H3C_SecCenter_CSAP_IQG-APW100/?CHID=365637

4. H3C SecCenter CSAP 产品 其余资料参考以下链接

   https://www.h3c.com/cn/Service/Document_Software/Document_Center/IP_Security/SecCenter/H3C_SecCenter_CSAP/?CHID=288332&v=612