关键信息基础设施中的网络安全运营研究

袁国伟

(国防科技大学 信息通信学院,湖北 武汉 430014)

摘 要:关键信息基础设施作为承载国家重要领域信息传递的载体,其安全关乎国计民生、公共利益和国家安全。近年随着《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》(以下简称"关保")等政策制度相继出台,关键信息基础设施网络安全已上升成为国家战略,引起社会广泛关注。因此,认清关键信息基础设施现实风险,设计基于态势感知的技术体系、建立合规的制度体系、构建权责分明的组织体系,实现人、技术、制度的有机结合,提升网络安全运营能力,对确保关键信息基础设施安全具有重要现实意义。

关键词:关键信息基础设施;网络安全运营;技术体系;制度体系

中图分类号:TP309 文献标识码:A DOI:10.19358/j.issn.2097-1788.2022.06.005

引用格式:袁国伟. 关键信息基础设施中的网络安全运营研究[J].网络安全与数据治理,2022,41(6):34-39.

Research on network security operations in critical information infrastructure

Yuan Guowei

(School of Information and Communication, National University of Defense Technology, Wuhan 430014, China)

Abstract: As the carrier of carrying information transmission in important national field, the security of critical information infrastructure is related to the national economy and people's livelihood, public interests and national security. In recent years, with the promulgation of the Network Security Law, the Regulations on the Security Protection of Critical Information Infrastructure and other policies and systems, network security of critical information infrastructure has risen to become a national strategy, which has aroused widespread concern in the society. Therefore, it is of great practical significance to recognize the real risks of critical information infrastructure, design a technology system based on situation awareness, establish a compliant system, and build an organizational system with clear responsibilities, so as to achieve the organic combination of people, technology, and systems, and thus improve the network security operation capability to ensure the security of critical information infrastructure.

Key words: critical information infrastructure; network security operation; technical system; institutional system

www.pcachina.com

0 引言

近年,国内重点行业领域加大信息化建设,构建覆盖多区域、多节点的广域网信息基础设施。在促进行业领域发展的同时,基于广域网体系架构、计算环境、边界防护的特殊性,关键信息基础设施存在诸多安全风险。2022 年 9 月 27 日,国家计算机病毒应急处置中心公告了美国国家安全局特定入侵行动办公室对西北工业大学的网络攻击行动,披露了其对我国关键基础设施实施攻击并窃取数据的事实。此次事件引起政府、社会和行业领域的广泛关注,加强关键信息基础设施网络安全防护成为各领域的共识。

1 网络安全风险及需求分析

1.1 基本情况

广域网是由不同地区局域网或者城域网连接而成的通信网络。随着信息化技术快速发展,很多政府部门、国防工业、大型企业等重点行业和领域通过光缆、卫通等链路,使用光传输系统、网络交换设备建立了专用的广域网。比如国家税务局构建了从总局到省、市、县四级广域网,各大银行构建了从总行到分行再到支行和营业点的专网网络[1]。

城域网结构通常采用"核心-汇聚-接入"分层结构,出口通过路由器连接广域网,依托保密机和防火墙等安防设备进行边界防护;核心层由多台

万兆交换机组成，进行业务的交换转发；汇聚层使用千兆交换机，连接不同的接入节点；接入层负责将终端接入网络，如图 1 所示。

1.2 风险分析

1.2.1 脆弱性分析

广域网基于其自身的特点，在保证重点领域和行业从总部到节点间的信息传递的同时，存在诸多薄弱环节。一是在对外联网方面，大多数行业领域需对外提供服务和业务，或由外部为本行业提供服务和业务，存在多节点对外联网需求，外部行业环境、人员、网络、终端不受控，接入方式各不相同，存在较大风险。二是在传输层方面，各节点内部主要依托光缆资源完成内部城域网或者局域网组网，总部至节点和节点间主要采用光缆资源和卫星通信构建广域网。其中光缆资源主要采取自建或者租用运营商链路，易被物理破坏或遭受自然灾害，进而导致通信中断；卫通链路鉴于其传输体制透明公开的特性，易受收到电磁干扰而导致中断。三是在用网设备方面，很多行业领域在网络建设初期未考虑安全防护要求，大量使用国外设备和操作系统，相关设备和系统存在很多先天漏洞，如未及时进行更换或者漏洞修复，极易被不法分子所利用。

1.2.2 威胁识别

基于重点行业领域的特殊地位和关键信息基础设施广域网复杂架构，根据威胁的属性，从自然威胁和人为威胁两方面进行分析。自然威胁方面，可能的威胁有地震、雷击、洪水、静电等；人为威胁方面，主要包括敌对国家、黑客组织、网络恐怖分子的网络攻击行为和内部工作人员的不安全网络行为，如表 1 所示。

1.2.3 存在的主要风险

广域网自身存在的脆弱性，使得自然和人为威胁存在造成安全事件的可能。通过上述分析，从内部和外部两个维度分析关键信息基础设施存在的主要风险。

(1)内部风险，主要包括人员操作、设备问题、信息安全防护等方面。一是人员操作方面，受限于人员用网安全意识不强，存在违规跨网传递数据、接入外

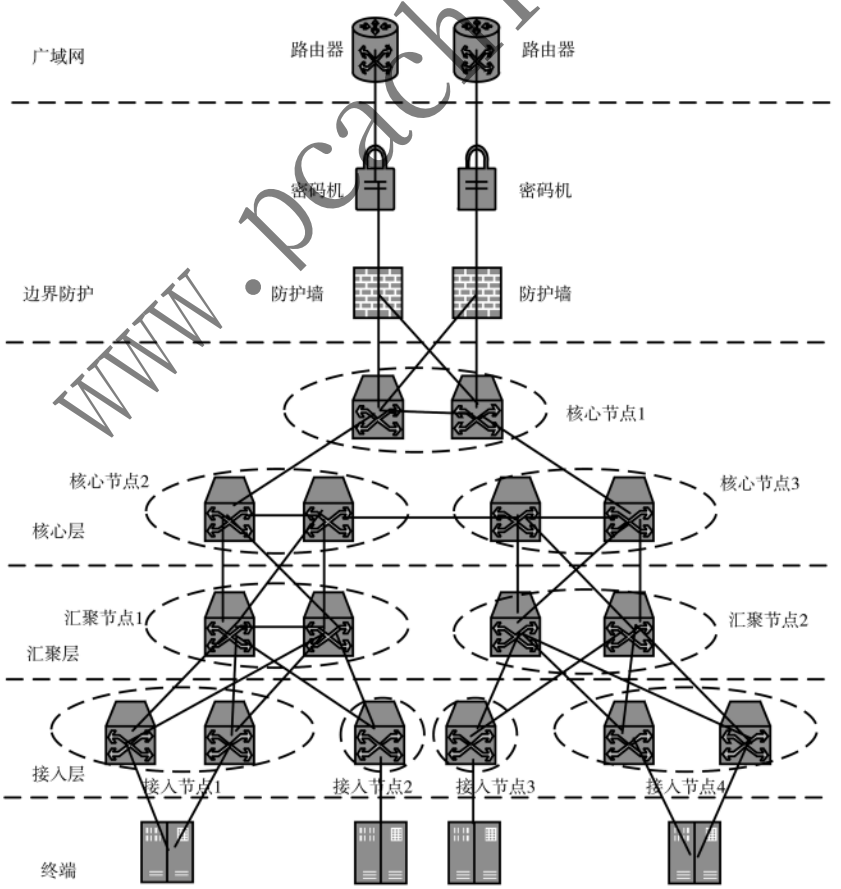

图 1 城域网拓扑

www.pcachina.com

表 1 威胁描述

威胁主体	描述
敌对国家	具有很强的目的性,通常成立专职网络对抗力量,使用专业的攻击手段和技术,窃取网内重要数据或者干扰破坏业务
黑客组织	攻击目标通常是随意的,由技术较强的人员组成,通常为个人兴趣或者利益驱使
网络恐怖分子	攻击具有一定的目的性,采取恶意植入木马、网络入侵等方式,意图谋求不正当诉求
内部工作人员	一方面因操作失误,导致网络遭受威胁;另一方面可能被串通、勒索等原因成为恶意攻击者

联设备导致信息泄露、病毒植入等风险。另外,由于运营人员自身安全运营能力不足导致安全事件扩散的风险。二是设备自身方面,由于用网装备开发、设计、生产和使用未考虑安全防护要求,安全管理设备自动化、通用化程度不高,加之日常管理不规范,从而因设备自身问题导致网络异常。三是信息安全防护方面,由于网内盗版软件、操作系统存在安全漏洞和病毒特征,存在被攻击、利用、嗅探的风险。

(2)外部风险主要体现在网络外联、自然灾害和敌对势力攻击几个方面。重点行业领域大多存在对外联网需求,存在因边界管控不到位而被不法分子利用实施网络攻击的风险。由于广域网主要依托有线、卫通链路组网,一旦遭受地震、雷击等不可抗力影响,造成某一节点或者链路受损,将直接导致网络中断。基于关键信息基础设施的特殊重要性,敌对势力易采取通信链路干扰、网络攻击、木马植入等手段,对其实施硬摧毁或者软杀伤,进而影响业务系统安全。

1.3 需求分析

1.3.1 网络安全运营

业界对网络安全运营的定义不尽相同,经过多年的理论研究和运营实践,核心思想趋于一致。这里参照《网络安全运营服务能力指南》[2],将其定义为以确保网络安全为目标,以资产管理为核心,以安全事件管理为关键流程,以安全态势感知为主要技术手段,进而协调各级组织和人员,开展安全审计、风险评估和事件处置等工作。其内容从技术和管理两个维度进行概况,技术层面具体包括资产监视、安全防御、监测分析、应急处置等相关内容;管理包括制度建立、机构设置、人员管理、运维管理等内容。

《中华人民共和国网络安全法》《网络安全等级保护条例》(以下简称“等保”)对广域网架构下的关键信息基础设施安全运营建设内容进行规定,明确关键信息基础设施为相关领域和行业遭到破坏可能危害国家安全、国计民生、公共利益的重要网络设施和信息系统。据此,关键信息基础设施按照“等保”定级指南,需按照三级及以上安全防护等级执行防控措施,并进行重点保护。这里从技术和管理两个维度,参照“关保”“等保”中的标准要求,结合网络安全风险实际,对网络安全运营建设需求进行分析,确保体系建设合规。

1.3.2 网络安全运营技术需求

“等保”“关保”围绕资产管理、安全防护、监测分析、事件管理等方面,提出开展资产梳理、加强边界监测、事件集中管理等标准要求,强调网络运营的主动防御、动态防御[3]。可以看出,关键信息基础设施网络安全运营技术体系建设上,需借助数据采集、融合分析、态势显示等态势感知技术,围绕资产监视、安全防御、监测分析、应急处置等流程,构建立体、动态的防御体系,形成覆盖全局安全态势,并与网络设备和运营人员进行有机联动,及时响应安全事件,实现网络安全的闭环管理[4]。

1.3.3 网络安全运营管理需求

“等保”“关保”围绕组织体系和制度体系两方面,就目标策略制定、组织体系建立、规章制度构建提出了具体标准要求。可以看出,关键信息基础设施网络安全管理体系建设上,需建立覆盖安全管理活动制度、规程、机制,明晰各级管理责任,通过规范化的人员培养,建立完备安全运维、检查评估、监测预警和事件处置流程,实现组织、制度、流程的体系化设计,为网络安全运营提供制度支撑[5]。

2 安全运营体系构建

2.1 体系框架

对照前述技术和管理需求,参照“等保”“关保”有关标准要求,围绕组织、制度、技术对关键信息基础设施网络安全运营进行体系化设计,通过构建规范化的组织体系、一体化的态势感知运营平台和系统化的管理制度规范,进而实现网络安全运营的体系化建设[6]。

2.2 网络安全运营组织体系

区分技术和行政管理,按照“谁主管、谁负责,谁维护、谁负责,谁使用、谁负责”的原则,建立包含决策层、管理层和支撑层、执行层的自上而下的组织体系(如图 2 所示)。

在总部设立网络安全管理委员会,作为决策机

www.pcachina.com

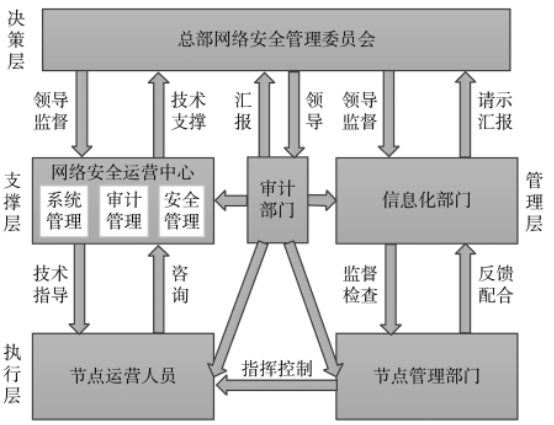

图 2　关键信息基础设施组织体系

构负责网络安全的全面工作，最高领导由总部网络主管领导担任，成员包含下属单位网络主管领导、总部信息化部门领导以及网络安全运营中心领导，下设办公室具体负责日常业务协调。管理委员会履行审批网络安全管理目标、安全制度、重大项目、工作报告，决策处置重大突发事件等职能。

总部信息化部门牵头负责总部安全运营管理工作，履行运营制度制定、网络事件指挥协调，并检查督导各级执行制度要求等职能。

总部网络安全运营中心负责总部的关键信息基础设施的安全工作，并负责为其他单位网络安全运营提供技术支撑。各下级单位网络管理部门承担本单位的网络安全主体责任，细化分级上级制度，并按要求调配运营力量，为主要执行力量。总部审计部门独立于网络安全管理组织和网络安全执行组织，强调事后审计，主要是对总部信息化部门和各级单位网络管理部门进行网络安全工作评价。

2.3 网络安全运营制度

如图 3 所示，制度体系上，以国家相关制度和标准为基本依据，由网络安全管理委员会审定网络运营总体目标、安全策略和安全保护计划，由信息化部门制定配套的安全管理制度，并由网络安全运营中心结合日常运营实际制定相应的运维机制，进而形成集策略方针、管理制度和运维机制于一体的制度体系，指导并有效规范各级开展网络安全运营工作。通过严格制度和发布、评审和修订，实现制度间的有效衔接和一致性。

2.4 网络安全态势感知和运营平台

2.4.1 设计思路

对照“等保”积极防御、主动防御的技术需要，突出应对关键信息基础设施的现实风险，依托一体化平台实现对网络安全运营资产监视、安全防御、监测分析、应急处置等活动的集中管理。系统主要围绕以下四种能力进行设计。

一是数据集中管控。在网络层和传输层数据的基础上，引入光传输系统、卫通、光缆监视平台物理

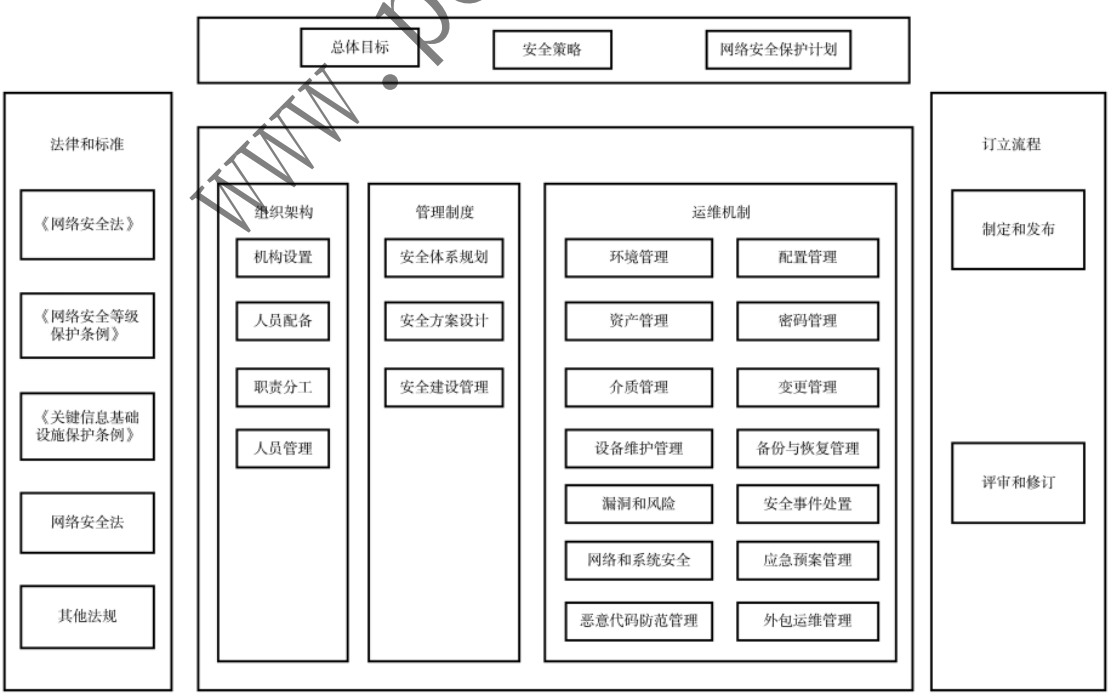

图 3　关键信息基础设施制度体系

www.pcachina.com

层数据,实现从物理层、网络层到传输层的数据集中采集和管理,为数据分析和态势展示提供多维度、成体系的数据资源。

二是分析决策快速高效。通过提取关键特征要素,依托攻击态势分析、节点出口监测、重点出口监测、重点区域监测、异常流量分析、访问行为等分析引擎,形成对关键安全域、异常情况的实时分析结论,支撑数据回溯分析和态势显示调用。

三是安全态势一体展示。建立多维度、全时段的网络安全态势呈现,满足指挥、管理和运维各类需求。能够按照网络区域、地理区域和网络安全事件等属性,提供网络拓扑、饼图、表格等多种呈现方式,为运营人员提供直观展示界面。

四是应急响应快速高效。通过构建应急预案、威胁库、情报库、经验知识库等各类知识库,事先对安全事件进行剧本编排,在人、设备、事件有机联动下,实现对网络安全事件的自动响应,缩减应急响应时间。

2.4.2 体系架构

针对上述技术建设需求和思路,为更好地应对关键信息基础设施的威胁和风险,参照态势感知技术模型和 SOAR(安全编排自动化与响应)模型[7],借鉴当前成熟的运营平台建设经验,构建集数据平台、分析平台、态势显示平台和事件处置平台于一体的态势感知和运营平台架构(如图 4 所示)。在对全网流量信息、资产情况进行全面收集、监测的基础上,利用分析层对数据进行融合分析,其后在显示层以可视化的界面呈现,进而为事件发现、溯源查证、安全运维和自动化提供技术支撑。

(1)数据管理平台

数据管理平台主要用于数据的采集和预处理,是其他平台的数据支撑平台,包含数据引接模块、数据组织与管理模块以及数据分析与服务模块。平台接入网络流量、安全设备、安管平台、资产信息和威胁情报的数据,并通过数据预处理形成安全数据资源库;其后通过各种汇聚关联模型对数据进行业务主题聚合,形成支持安全业务分析的主题数据库,供业务主题调用。

(2)数据融合分析平台

数据融合分析平台利用数据管理平台引接的数据,结合网络拓扑绘制、风险告警标绘等,通过多维分析、关联分析、流量分析、行为分析等数据分析引擎,构建包含安全风险、安全防护、安全策略、安全状态评价模型,实现对网络安全状态的评价指标管理、评价模型管理和评价任务管理。

(3)安全态势显示平台

安全态势显示平台依托数据管理和融合分析

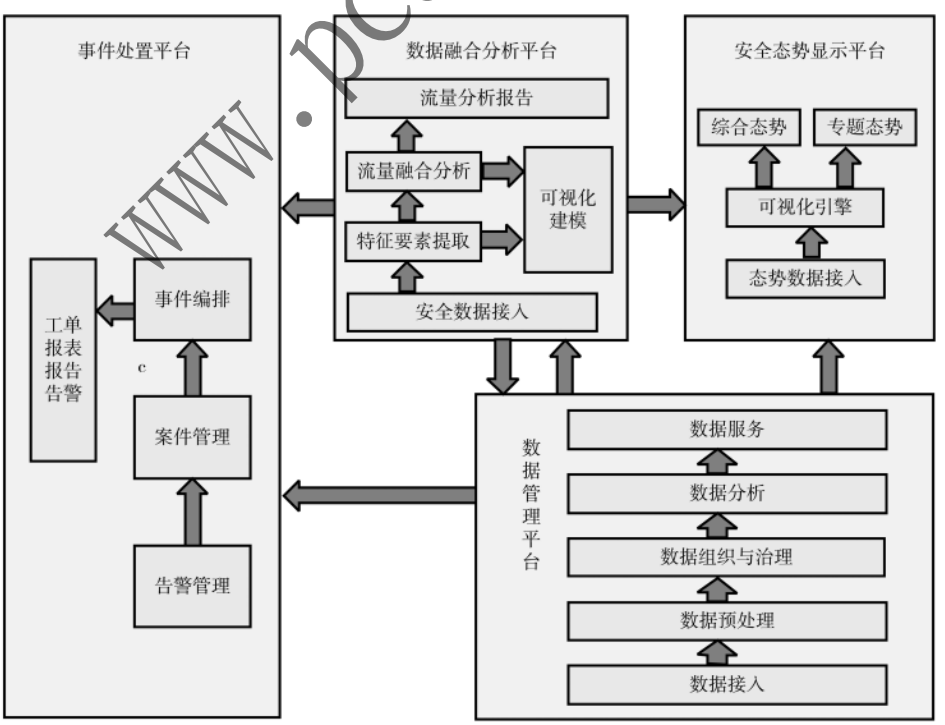

图 4 网络安全态势感知和运营平台架构

www.pcachina.com

平台，提供数据和分析支撑环境，通过图层的叠加组合，从网络综合安全状态(如表2所示)和业务域专题安全状态(如表3所示)两大视角系统显示安全状态信息和各类安全专题信息。平台以3D可视化技术为基础，以图层叠加方式显示各类安全状态信息和安全专题信息，以专业视角对各类网络风险和防护情况进行评估和呈现，对各类网络专题态势进行综合显示。

(4)事件处置平台

事件处置平台基于SOAR设计理念，从数据管理平台和数据融合平台获取安全事件信息，通过事件编排，生成对应处置策略，与运营人员和设备进行有机联动，实现安全事件的自动响应[8]。

3 结论

本文从关键信息基础设施安全风险着手，以网络安全可靠为出发点，着眼安全运营合规化建设，提出构建集人、技术、机制的一体化安全运营体系。基于态势感知技术、制度体系、组织体系建设来提升网络安全运营能力。网络安全运营作为一个复杂的系统工程，需要各级持续发力、久久为功，充分运用云计算、大数据等先进技术，打通各系统、各区域的堵塞点，实现网络安全的积极防御、主动防御。

参考文献

[1] 赵泽文.广域网网络安全防御综述[J].科技广场，2015(3)：117.

[2] 范渊.网络安全运营服务能力指南[M].北京：电子工业出版社，2022.

[3] 王斯梁，冯暄，蔡友保，等.等保2.0下的网络安全态势感知方案研究[J].信息安全研究，2019，9(9)：830.

[4] 马力，祝国邦，陆磊.《网络安全等级保护基本要求》(GB/T 22239－2019)标准解读[J].保密科学技术，2019(7)：15.

[5] 王斯梁，冯暄，蔡友保，等.等保2.0下的网络安全态势感知方案研究[J].信息安全研究，2019(9)：829.

[6] 张敬，李江涛，张振峰.企业网络安全建设最佳实践[M].北京：电子工业出版社，2021.

[7] 张健，董升来.基于SOAR模式安全运营建设的探索与思考[J].广播电视网络，2022(5)：57.

[8] 赵粤征，叶建伟，员珊，等.基于SOAR的安全运营自动化关键技术构建及未来演进方向[J].工业互联网安全，2021(40)：19.

(收稿日期：2022－09－30)

作者简介：

袁国伟(1990－)，男，本科，主要研究方向：通信运维管理。

表2 网络综合安全状态显示

功能区	显示内容	支持方式
整体安全状态	以网络拓扑形式显示整体安全状态和变化趋势，动态显示总部和各节点和安全状态排名	实时显示
网络安全风险状态	显示终端情况、网内弱口令情况、病毒告警情况、异常流量告警等	实时显示，支持导出报表
安全防护状态	监视网内网络攻击监测分析系统、终端防御系统、防护系统、防火墙、主机管控系统等设备的CPU、内存、硬盘存储、连通性等以及防护设备建设、人员分布等	实时显示

表3 网络综合安全状态显示

功能区	显示内容	支持方式
事件和告警专题	异常流量告警、威胁检测系统告警、病毒告警、防火墙阻断日志告警等	支持按照周、月、年显示查询； 支持到处报表功能； 支持下钻至告警详情 支持显示告警处置情况(未处置、处置中、处置完结等) 支持按单位及性能告警数量排序、告警次数排序、存在事件排序等
响应与处置专题	响应和处置效果跟踪和历史查看以及攻击还原	实时显示，支持导出报表
网络资产状态	显示网内资产信息，支持按照单位和地理区域划分，并按照人工方式研判后的告警事件排名	实时显示，支持导出报表，可支持点击下钻至具体设备信息

www.peachina.com

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com