基于大数据的网络安全态势感知关键技术研究

王　昕
汉江水利水电（集团）有限责任公司　湖北武汉　430048

摘　要：随着大数据、人工智能、云计算等信息化技术的发展，以及“网络空间安全”上升到国家战略层面的高度，网络安全态势感知也成为网络安全领域的新热点。利用大数据相关技术对网络运行相关海量数据进行分析、过滤、融合、识别已知和未知的安全威胁，建立完善可靠的安全体系，指导网络安全运维工作，从而有效保障网络安全。

关键词：大数据；网络安全；态势感知；关键技术

引言：

网络安全态势感知是相关的技术人员利用人工智能技术或者大数据技术等从大量的数据当中发现存在安全威胁的数据，方便于技术人员及时杜绝威胁网络信息数据安全的问题出现，创建稳定安全的网络数据运行环境，维护网络秩序的稳定以及安全，强化网络信息数据安全威胁的应急响应能力，做到对于网络系统的宏观把控。因此本文对于大数据背景下网络安全态势感知技术进行研究。

一、基于大数据网络安全态势感知的重要性

大数据的应用伴随而来的网络安全问题已经威胁到数据的安全以及国家网络的安全，近年来科技在发挥正面积极影响的作用的同时网络安全事故也在不断的发生，不利于良好网络秩序的建立，而随之出现的网络安全态势感知的概念引起了相关技术人员的重视，网络安全态势感知是相关的技术人员利用人工智能技术或者大数据技术等从大量的数据当中发现存在安全威胁的数据，方便于技术人员及时杜绝威胁网络信息数据安全的问题出现，创建稳定安全的网络数据运行环境，维护网络秩序的稳定以及安全，强化网络信息数据安全威胁的应急响应能力，做到对于网络系统的宏观把控。网络安全态势感知基于多源数据融合技术，通过收集网络运行中各种防御工具信息数据，并对这些信息数据进行融合处理，准确认知和判断网络运行现状，分类网络攻击行为，预测网络未来一段时间的运行状态，进而提前防范可能存在的网络攻击。在大数据网络安全态势感知平台中应用效果的考量，技术人员需要从整体上对安全态势感知平台的技术架构、数据存储处理以及分析等梳理，逐步明确数据融合技术应用的主要领域，为后续相关技术活动的开展提供方向性引导。网络态势感知能够在大数据的支持下，实现对设备运行状况、网络行为以及用户行为实时状态与变化趋势的有效解读以及科学预测，将大量无序的安全数据信息进行简化处理，从而实现对各类网络安全威胁的快速识别以及准确预测。在很大程度上弥补了过往大数据网络安全体系在安全防护方面存在的问题，增强了安全防护的针对性、有效性，大大降低了安全风险，为用户营造出安全的网络空间。

二、大数据网络安全防护面临的困境

随着网络科技深入各行各业，网络安全问题也愈加凸显，因此做好网络安全的维护工作，解决网络安全问题成为相关网络技术人员的研究课题。网络防护技术在科技的推动下在不断的升级以及完善，但在实际的网络防护技术使用当中依然存在着不同类型以及不同程度的网络攻击现象，出现了不同类型的网络系统漏洞问题。而传统使用的网络防护模式基本上主要是维度化防控模型，系统自检以及数据防控模型等，此种主要的网络防护模式也是目前最主要的防护体系。从网络技术角度进行分析，可以看出目前为止并没有一个最为安全的网络系统，不同的网络系统都会存在着不同程度的网络漏洞问题。针对目前网络安全维护工作存在的不足主要是采取被动防护，即当网络数据数道安全威胁时，相关的技术人员才能够根据网络安全威胁问题进行分析，根据分析结果来制订相应的网络安全威胁抵抗方法，并没有采取有效的方法攻击病毒，同时也是以被动的防御为主要模式来开展防护体系的更新，因此也给予了黑客进行防护体系攻击的更多机会以及漏洞。以往的防护体系存在的安全问题原因在于，对于数据信息没有同时开展传输，同时相关联的模块也没有及时的进行响应，以计算机系统数据中心为主的系统运行核心，在系统体系内存在其防护功能，并不能够感受到外界的危险；没有实现智能

化进行数据信息结构的创建，只是对于数据信息依照设置好的程序开展数据信息的构建，致使了建立的网络防护体系只是被动的防御方式，没有匹配度足够的数据信息，不能够具体的朔源分析网络防护体系受到的攻击。只是按照网络防护体系预先设定完成的机械化防护手段来应对，使得网络防护体系在长期的网络攻击下，出现系统漏洞的概率大大增加。

三、基于大数据的网络安全态势感知关键技术分析

1.建立态势感知指标体系

从大数据网络安全态势感知平台建设经验来看，为确保实际的处理效果，打造完整、高效的态势感知指标体系，研发人员需要对态势感知指标体系进行构建，通过指标体系来保证数据采集、数据预处理的关联性以及真实性、准确性。在这一思路的指导下，技术人员需要做好网络运脆弱子态势以及攻击子态势的评估工作。具体来看，网络运行脆弱性子系统主要用于分析评估网络中主机存在的漏洞以及安全情况，并以此为前提，对主机硬件配置以及软件系统安全漏洞的扫描结果报告、外部威胁报告等进行汇总。网络攻击子态势主要评估网络中主机遭受攻击的频次以及危害程度，涉及到SQL注入攻击次数、非授权扫描次数以及安全事件引发的危害度[1]。目前子态势数据主要来自与IPS、IDS以及防火墙等。异常行为子态势主要针对于各个主机内部，不同用户登录与访问过程中所产生的异常行为，其数据来源主要是4A系统以及相关日志，通过对指标体系的构建，将整个安全态势感知平台中的各类安全数据进行了融合，增强了态势感知的系统性与全面性[2]。

2.安全数据采集

采集网络安全数据主要通过3种途径：第一种是采集安全设备和业务系统的数据，这些数据涵盖的范围比较广泛，如防火墙、4A系统、入侵检测、堡垒机、安全审计、Web访问日志等，数据的数量非常庞大和复杂；第二种是采集运行维护管理过程的数据，比较常见的如故障处理信息数据、安全风险评价结果、安全巡检情况、安全管理体系运行记录等；第三种是采集外部威胁情报库，包含攻击网络系统的来源、具体的攻击行为特征、域名、漏洞等各种信息数据。

3.对数据进行预处理

通过数据采集可以得到一些安全数据，这些都是非结构化数据，有着价值密度低的共同特点。因此须事先做必要处理，才可以对有价值的数据进行有效识别和修复，并及时删除存在重复、错误的数据，当完成以上操作才可以继续开展后期的数据挖掘工作。经过预处理后的数据，在进行统一存储时可以采用自定义的格式。如果出现不同来源的数据，要及时进行标注工作，含设备的来源、时间等。如果在不同设备中发现同一时间的记录信息，可以将其进行合并处理，并删除重复的信息。如果发现由于误报产生的孤立安全事件报告，可以采取重新清洗的方式进行处理。一般来说，经过预处理后的数据，价值密度会得到较大提升，有助于提升数据后期挖掘和分析工作效率。

4.异构融合技术

在进行网络数据信息的传递时，多个系统会供应日志的种类和日志的数量等，不过由于不同系统拥有不同的特征，导致了数据信息的各项行为参数的差异性明显存在，由于不存在与此相适应的基准处理参数，为此对于结合在一起的日志数量进行整体化解读时，则极有可能解读出不准确的信息数据。而态势感知技术通过多样化的网络运行体系，对于日志数据的原有格局进行打乱，将日志数据的格局创建成为水平，垂直交叉特性的格局，使得最终形成的数据信息能够成为一个整体，之后再借助检测技术整体化的检查相关数据信息[3]。此种方式可以有效的提高对于数据信息的检测效率，实现对于每一个链块，每一个字节等细节的有效检查，使得最终的数据信息检测结果具有准确性以及全面性。

5.态势预测工作

在进行态势的预测时，会应用一些数据融合算法，如灰色数据模型、自回归移动平均模型等。借助于数据融合算法，可以更直观地反映出态势的变化。在实际的预测过程中，需要找出原有的态势数据并对其进行分类。按照形式区别分为两类：输出数据和输入数据。为了使输出数据的数值渐渐接近输入数据的数值，可以适当调整模型参数，最终得到可信度较高的初步预测模型。在初步预测模型的基础上，将机器学习的方式运用其中，从而得出相对完善的预测模型。

6.决策技术

可视化技术是指在借助数据信息的运行模式的情况下，使得技术人员可以对于数据模型再借助建立的立体框架的情况下，使得对于数据模型的解读更加直观化。第一阶段是进行数据的转换，对于相关数据进行管理检测，之后将处理过的数据进行表格化转换，可以根据系统本身具有的实时化特点，使得对于数据的映射过程可以在极短的时间内完成，之后在完成数据映射流程之后，

之后按照系统预设的方式将完成数据映射的数据信息进行创建以及存储。第二阶段是数据的图像映射，此阶段是对于已经形成的数据表格按照系统设置的参数图像进行映射，并且借助信息搭载平台，实现对接以及转换数据表格[4]。第三阶段是视图转换阶段，实现以空间坐标为主的数据转换，在确认某一项数据参数之后创建图像模型，根据图像映射得到的数据信息实现对于数据信息的系统自动性调整，例如按照颜色比例格，局以及位置等信息进行调整，使得数据信息能够在各项参数的规划下进行视图转化。

四、结束语

综上所述，态势感知的部署，对于机构内部网络安全统一管理，掌握网络安全状况，为网络安全优化提供决策依据具有重要意义。不断增强大数据网络安全态势感知平台的建设效果，在弥补过往网络安全防护体系缺陷的同时，形成现代、安全、高效地实时防护系统。

参考文献：

[1]戴祥华，张苏炯.大数据网络安全态势感知中数据融合技术的研究[J].中国信息化，2020（4）：81-82.

[2]邓晓东，何庆，许敬伟，等.大数据网络安全态势感知中数据融合技术研究[J].网络安全技术与应用，2019（8）：79-80.

[3]董超，刘雷.大数据网络安全态势感知中数据融合技术研究[J].网络安全技术与应用，2019（7）：60-62.

[4]韩晓樱.浅谈网络安全态势感知系统及其关键技术[J].电子世界，2019（11）：206.