基于大数据的网络安全态势感知系统应用于网络安全管理中的研究

罗嗣扬
上海英夫泰尔克软件开发有限公司　上海　200233

摘　要：在大数据、互联网技术、云计算等信息技术的发展背景下，互联网技术在人们的生活和工作中得到了广泛的应用，对于网络的攻击形式和手段也越发多元化。有效运用网络安全态势感知系统，可以进一步提高对内部与网络攻击源的定位和处理效果，根据宏观视角有效评估影响以及理解其中的意图，就此提供相应的决策支持，提升网络抗风险能力，达到当前网络安全管理的要求。

关键词：大数据；网络安全管理；态势感知；技术

Research on network security situation awareness system based on big data applied to network security management

Siyang Luo
Shanghai Infortech Software Development Co., Ltd, Shanghai, 200233, China

Abstract: Under the development background of information technology such as big data, Internet technology, and cloud computing, Internet technology has been widely used in people's life and work, and the forms and means of network attacks are becoming more and more diversified. The effective use of a network security situational awareness system can further improve the position and processing effect of internal and network attack sources. According to the effective evaluation of the impact and understanding of the intention from a macro perspective, we should provide corresponding decision support, improve the network's anti-risk ability, and meet the requirements of the current network security management.

Keywords: big data; Network security management; Situational awareness; technology

前言：

在信息技术、大数据技术、移动互联网技术的发展背景下，人们的生活和工作早已离不开这些互联网技术的支撑，并且对于互联网的攻击方法越来越多元化，特别是近年来的挖矿软件的增加，携带病毒的软件愈发泛滥，严重影响着全球网络安全。如果只是采用单一的安全保护方法，已不能达到目前网络安全管理的相关要求，对此需要建设统一的网络安全管理系统，综合评估和分析网络安全日志，以此提高网络安全管理质量，在这样的情况下，应用态势感知系统的意义越发明显。态势感知系统时基于互联网技术而形成的检测系统，能够全面、动态式的预测安网络全风险，并通过大数据和安全相关的技术，增强安全责任方对安全风险的识别能力以及应对水平。在深层次的分析中，检测正常使用者和入侵者之间的不同，识别其中的潜在风险，更加精准的掌握信息系统中出现的异常，并就此作出合理的管理决策。比如应用态势感知，可以在攻击行为中检测攻击者的目的和使用的手段，以此深入分析系统损伤的原因。

1　网络安全管理的新标准

1.1　24h全面监测体系

搭建实时全面监测体系，能够全方位监测内部网络的安全情况，分析全部流量威胁，围绕网络脆弱性、外部攻击性以及内部的异常三大维度来建设全面监测体系。这三大维度有着自己对应的终极目标，其中脆弱性的核心是业务资产，并以此寻找暴露面；外部攻击性是探究攻击突破弱点和攻击环绕情况，根据脆弱感知来优化和调整预防方案，以此加固决策方向；内部的异常时探寻已经被入侵成功的主机以及其中潜在的安全风险，以防

系统不断受到损害[1]。

1.2 攻击溯源

攻击溯源在网络安全事件的管理中发挥着重要的推动作用。如果出现网络安全事件，则可以对日志进行全方位的分析，第一时间探寻安全事件中的问题，就此展开全面的分析摩西，能够有针对性的分析并处理安全事件发生的路径以及更多的相关内容，从而精准定位和溯源攻击者，并采取有效的应对措施。

1.3 安全管理

安全管理是24h全程监测和保护网络环境，其关键点是着重管控基础信息。对于网络内部的相关数据和应用，需采取相应的管理和保护，在网络资产的整理中，设置相应的保护目标和具体方式，结合核心网络资产开展实施监测和预警工作[2]。

2 网络安全态势感知系统能力

在网络安全管理中运用态势感知系统，该系统可以全面监测网络安全形势，其系统内部必须要具备机器学习能力和自动发现问题的能力，比如可以对网络资产，攻击行为等进行全面的统计类态势感知，同时能够感知攻击性为的挖掘类态势。在人机交互中，不断提高识别结果的精准度，优化和学习先进的分析结果，构成良好的感知数据分析[3]。

2.1 网络安全可视化

网络安全态势感知平台最重要的能力体现在网络安全可视化，也就是网络安全态势感知系统面向外部环境和用户提供网络安全预警，安全事件和态势分析结果的窗口，该窗口提供的信息和用户的网络安全管理业务要求有着紧密的联系，网络安全可视化进一步丰富了系统功能，在这样的背景下，将网络安全可视化呈现能力问题统一化[4]。通过网络安全信息呈现窗口，充分展现了网络资产分布、态势分析、各种事件的排名，还有安全警告等信息内容，让用户在充分的信息分析中精准定位并处理好网络安全问题。

2.2 网络资产整理

在精心的部署探针下，运用扫描技术和爬虫技术开展主动探测工作，以上网行为管理、限制和无限介入控制系统的用户同步功能为辅助，以此搭建一个完整的知识库，从而获取真实有效的在线设备资产，最后借助大数据分析技术，快速获取目前在线设备的总数量，包括历史设备接入情况。

2.3 资产脆弱性感知

网络安全管理的重要保护要点就是网络资产，特别是承载业务服务器资产，该服务器脆弱性也就是服务器弱点，每个服务器本身就存在着弱点，任何的威胁和攻击都会利用这些弱点进行侵入和伤害，对此，服务器脆弱性的感知和优化对网络安全管理来说有着重要意义，这样能够防范安全风险的产生。脆弱性感知能力要拥有分析内网资产的脆弱性的功能，包括了配置风险、弱口令、Web明文传输以及漏洞等方面，需要快速定位，从而精准分析其资产IP信息，直接勘察服务器存在的弱性风险，脆弱性风险以及热点漏洞等信息，在主动被动作用下，根据脆弱性指纹信息，加快聚焦服务器存在的信息和数据，为运维人员提高维护依据，以此能够快速定位，准确处理。

2.4 文件威胁监测

文件威胁在攻击链中是重要的发起手段，病毒文件主要是通过网站挂马、钓鱼邮件等方式进入内网主机，其恶意文件会在用户主机运行时，主动连接控制端，之后进行邮件发送，致使主机被控制，或其中的敏感数据被盗取，文件威胁属于内网横向攻击发起的头，态势感知系统会深入分析网络流量的基本情况，整体呈现文件威胁形势，从而准确定位威胁源头[5]。

2.5 日志关联分析

大量收集第三方产品SYSLOG日志，操作系统的日志信息，从而进行关联分析，综合分析第三方安全信息和事件日志，直接为用户呈现接入设备情况、数据信息，安全事件统计情况，关联统计、日志统计和日志传输情况，让用户能够准确定位各个设备的运作情况[6]。

2.6 攻击行为态势感知

网络资产每天会遭受各种冲击，并且这些冲击是客观存在的网络攻击，也许是来自于系统自身的漏洞，导致内网面临着各种威胁警报和潜在风险，致使IT运维逐渐复杂化，对此，在开展安全监测功能性分析时，要实时学习、归纳、监测全网个攻击行为，同时借助大数据技术充分分析木马攻击行为，以此准确识别和定位真正的攻击行为，在大数据技术的分析中，构建成精准、直观的分析形式，形成直观化的展现方式。

3 态势感知系统运行原理

态势感知系统，也是一种数据管理系统，涉及了数据采集、保存、分析和呈现，并且需要详细管理好每个环节。另外，还需要运用各种数据处理方式，关联分析不同的异构源数据信息，并使用可视化的展现方式，以此充分运用交互方面的功能性。

3.1 数据采集

大数据在分析之前需要进行数据采集，只有确保数据信息的质量和真实性，才能保证安全分析结果的有效性。对于不同的业务应用和网络环境，还有用户对态势感知场景的需要，借助数据采集对象和收集到的内容，设定专门的分析场景和建设模型。对于网络设备、应用、主机、安全设备等记录的告警信息和日志数据；反常的流量数据和在规则要求下匹配好的网络流量数据；还有整个网络中的人员、资产、漏洞和账号信息，以及威胁信息和脆弱性信息等，为了提高态势感知的场景化，为数据分析提供相应的数据支撑，采用建设特征库、漏洞信息库的手段，全方位提高各个网络节点的对比分析功能。在用户实际运用中，就可以结合上述功能，了解网站数据信息的变动[7]。

数据采集的关键点就是通过设备自带的探针功能收集相关信息，采集相应的数据需要借助各区域交换机镜像口收集镜像流量，并在此基础上全面分析相应数据信息，对于数据采集口的规划必须要全面、科学。在网络安全管理的要求下，一个比较安全的网络拓扑经历了详细的分区，最少也包括了用户区、运维管理区、服务器区一级其他机构互联网区，具有一定条件的还可以进一步细化分类，数据采集口的规划要求要尽量涵盖所有的区域，最好要全面获得每个区域的流量信息，同时整理各个安全设备的日志内容，以此为态势感知系统的大数据分析提供功能支撑。

3.2 大数据分析

3.2.1 数据预处理

数据预处理主要有三个阶段，其一是数据清洗，也就是通过数据标注和数据规则匹配来清洗原来的数据，以此提高数据的精准度和安全性；其二是数据的融合，把基本的安全数据根据已知的特点进行整合，以此形成拥有同样特点和属性的数据组。最后，数据关联，根据IP关系、交互特点和时序关系等将相应数据关联起来，构成基本的数据关系网络图[8]。

3.2.2 数据标准化

数据标准化是在原始数据中提取各类不同属性的数据信息，将原来的数据转化成同一标准的数据信息，以此为后期的数据分析提供相应的数据结构。收集到的数据源中包括了网络流量、交互IP、目标端口、用户行为等数据信息，这些数据体现了统计特点是可以明确表述同一个网络工作，如果使用传统的策略控制方式，是无法探测出这个网络工作的。大数据分析最常使用的数值统计方式，见图2。一些统计结果无法完整且准确的判断明确具体的网络行为，但是在整体分析而言，能够在大量的数据中发现异常，同时可以准确找到重点线索，方便后期的深入分析[9]。

表1　统计方法

统计方法	可能的网络行为
（某一时间段内针对IP、端口的）访问次数统计	网络扫描、嗅探
访问深度统计	网络爬虫、网站遍历
访问宽度统计	网络扫描、猜测后台登录地址
Agent连接数	弱口令猜解、扫描
Get文件访问比例	网站遍历
非静态文件访问比例	CC攻击
非200请求比	异常流量、数据泄露
……	……

3.2.3 可视化呈现

可视化的呈现的关键就是处理、溯源和告警，可视化展示的态势感知系统将会为用户展示最直接的内容，预警体现了数据分析的应用情况，是在数据分析结果支撑下，进行网络安全事件告警，形势分析、安全预警以及追踪溯源等使用。充分运用采集到的数据进行统计分析、关联分析、数据挖掘和能力评估等，构成可视化呈现需要的安全风险态势、安全运行态势以及网络风险态势等基础信息。

通过这些数据的深入分析结果，全面根据态势关联，网络危险情报等，对其进行有效的合成，以此得到网络安全指数，提取攻击手段，还远攻击全过程，追溯攻击者，对用户展示完整的数据信息，让用户具备充足的数据支撑进行安全事件的处理和应对。良好的可视化界面能够快速有效的探寻网络中的溯源和风险，以此及时应对和处置，很多态势感知系统会具备相应的防火墙联动处理方案，以便用户可以运用态势感知系统优化防火墙规则，从而进行联动处理，这一功能只对同一个牌子起着良好的兼容作用。

4　建设网络安全态势感知系统

网络安全态势感知系统一般情况下会将防火墙、安全审计系统以及杀毒软件等数据信息系统集合起来，以此评估整个网络现状，并在此基础上预估未来发展形势。该系统主要包括四个方面，即数据采集、特征提取、态势预测以及安全防护预警。

对于网络安全威胁数据采集，需要全面感知数据源，同时借助大数据技术建设高质量数据库。首先从安全角度出发，在明确网络攻击情况时，要进一步确定每个阶

段的基本情况，比如违规操作、恶意代码等，另外要收集其中的不良特点，实行有效的防护措施，以此为后期是管理工作打下基础。其二，对于数据的保存和管理方面，要构建科学的文件系统，同时根据相关标准保证该系统中的数据信息达到要求，以此从本质上达到实时传输数据的目的。

对于特征提取方面，需要多角度、多层次的开展工作。比如可以结合网络业务安全、数据安全以及基础设施安全等网络安全整体因素进行提取，根据不一样的场景和规模选择不同的方式。

对于态势预测方面，需要具备更加丰富的逻辑推演和数据搭建能力，能够结合不一样的评估结果精准预测相应的发展趋势，以此预防重大安全事件的产生。

对于安全防护，要通过可视化的形式展现各种网络安全形势，为每个系统和用户提供交互可能，并且可以按照不一样的标准自动形成相应的安全评估报告。

5 结束语

在互联网技术的快速发展下，网络安全工作将面临着更高的要求，在网络文件和病毒等风险威胁下，网络安全管理者将会面对更多的挑战。当网络安全事件一旦产生，该怎样准确定位攻击源，进行有效的应对措施，将损失降到最低，这些都是网络安全管理的基本，因此在管理工作中有效运用态势感知系统对于安全运维人员来说有着重要意义。

参考文献：

[1]刘冬兰，刘新，张昊，等.基于大数据的网络安全态势感知及主动防御技术研究与应用[J].计算机测量与控制，2019，27（10）：5.

[2]强常军.网络安全态势感知在铁路客票信息安全的应用[J].自动化与仪器仪表，2022（1）：4.

[3]宾冬梅，杨春燕，余通，等.基于深度行为分析的网络安全态势感知技术[J].微型电脑应用，2022，38（1）：4.

[4]郑攀，陈臣.网络安全态势感知探索与实践[J].中国数字医学，2021，16（6）：5.

[5]焦萍萍.大数据挖掘在船舶通信网络安全预警中的应用[J].舰船科学技术，2020，v.42（06）：122-124.

[6]赵志岩，纪小默.智能化网络安全威胁感知融合模型研究[J].信息网络安全，2020（4）：7.

[7]张艾森.无线通信网络安全态势识别方法研究[J].自动化仪表，2022，43（2）：5.

[8]尹彦，张红斌，刘滨，et al.网络安全态势感知中的威胁情报技术[J].河北科技大学学报，2021，42（2）：10.

[9]糜旗.网络安全态势感知平台架构设计[J].兵工自动化，2021，40（1）：5.