 DOI: https://doi.org/10.26549/bdai.v4i6.15245

Design of Information Security Situational Awareness System Based on Artificial Intelligence Technology

Wei Wang Yafeng Wang Shan Huang

College of Big Data and Artificial Intelligence, Shaanxi Technical College of Finance & Economics, Xianyang, Shaanxi, 712000, China

Abstract

With the continuous development of network technology, the problem of network security is becoming increasingly prominent. Therefore, network security situation awareness, as an active and comprehensive security technology of defense, has important practical significance. In order to strengthen the network information security protection, improve the security and reliability of the network, this paper based on artificial intelligence technology, the information security situational awareness system hardware design, and build the security situational awareness architecture, introduces the composition of security situational awareness system structure, finally to the security situational awareness system system test. The test shows that the security situational awareness system can maintain a relatively stable low response delay, and has good performance and certain application value.

Keywords

artificial intelligence; information security; situational awareness

基于人工智能技术的信息安全态势感知系统设计

王伟 王亚凤 黄珊

陕西财经职业技术学院大数据与人工智能学院，中国·陕西 咸阳 712000

摘 要

伴随网络技术的不断发展，网络安全问题日益突出，因此，网络安全态势感知作为一种主动防御的综合性安全技术，具有重要的现实意义。为了加强网络信息安全防护，提高网络的安全性与可靠性，论文基于人工智能技术，对信息安全态势感知系统进行硬件设计，同时搭建安全态势感知架构，介绍安全态势感知系统的组成结构，最后对安全态势感知系统进行系统测试。经测试表明，该安全态势感知系统能够保持较稳定的低响应延时，具有良好的性能和一定的应用价值。

关键词

人工智能；信息安全；态势感知

1 引言

人工智能技术作为一种综合性技术，涵盖多个领域，如深度学习、机器学习等，通过使用深度学习与机器学习等技术，有助于帮助系统更快地识别与应对未知威胁，从而提高安全识别与监测的能力，与此同时，人工智能技术不仅能够实现自动化处理与响应，还能够长期分析大规模安全数据以做到实时预警与防御，将人工智能技术合理应用到安全态势感知系统中，可以实现智能化监测、处理、防御以及预警，有效降低安全风险与损失。

2 硬件设计

2.1 Syslog 告警日志采集器

Syslog 告警日志采集器作为重要的信息安全工具，主要负责收集、分析与监测系统日志信息，综合应用人工智能技术与态势感知技术来快速识别网络中潜在的安全风险与威胁，从而构建全面的安全态势视图 [1]。采集器采集到的数据由态势评估模块进行评估，流程是先量化处理数据样本，而后利用人工智能技术来训练分类模型，结合相应指标来评估态势样本，接着计算出态势值，并将结果存储到预测中心，如此完成一次网络安全态势感知。此外，该采集器具有一定的可扩展性与灵活性，能够针对不同的安全需求进行相应调整，其应用范围广泛，适用于收集、分析与监测应用程序、网络设备及操作系统等多种来源的日志数据信息，为计算机网络的信息安全防护提供有力保障。

2.2 NetFlow 网络流量采集器

安全态势感知系统需要持续采集网络内部的安全流量，通过实时收集与分析网络中的流量数据，以及时识别与发现潜在的安全威胁，因此，选用 NetFlow 网络流量采集器来采集、监测和分析内部流量。此外，该采集器因灵活的配置扩

【作者简介】王伟（1979–），男，中国陕西西安人，博士，高级工程师，从事计算机、人工智能、大数据研究。

展性与强大的数据处理能力而被广泛应用于多种安全需求和网络环境中，为网络信息安全保驾护航。

3 网络安全态势感知架构

网络安全态势感知作为一种主动防御的综合性安全技术，旨在通过综合分析网络中的流量与事件来实时感知与预测网络未来的安全状况与安全趋势，以及时发现与应对潜在的危险与威胁。其核心要求是实时、全面、准确地采集网络中的安全态势数据，同时结合感知信息处理与态势可视化需求，设计出网络安全态势感知架构，如图 1 所示。

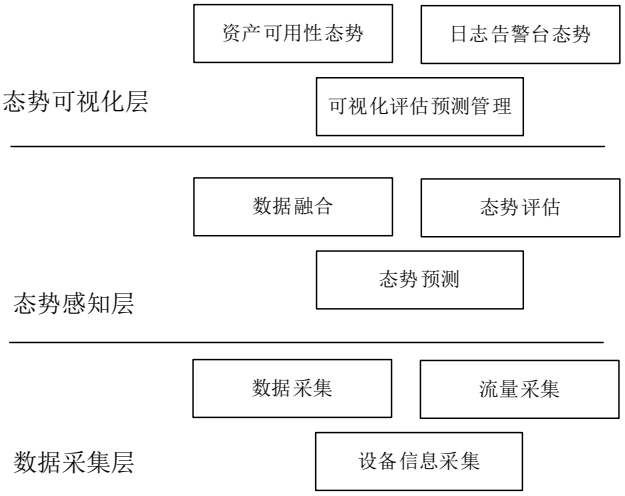

图 1 网络安全态势感知架构

如图1所示的网络安全态势感知架构包括数据采集层、态势感知层以及态势可视化层。数据采集层负责收集网络中各种数据，综合利用多种技术手段，如网络流量采集、设备信息采集及数据采集等来采集网络中的流量数据、日志数据、事件数据等，该层还具有一定的数据预处理与过滤的能力，能够去除无效或冗余数据，保留有价值的数据。态势感知层是整个态势感知架构的核心部分，具有数据融合、态势评估与预测的功能，负责处理与分析来自数据采集层的数据，同时能够识别、评估与预测网络中的攻击模式与安全威胁，该层基于人工智能技术，具有强大的机器学习能力与数据处理能力，可以快速处理与分析高复杂度、大规模的数据，与此同时该层还具有安全事件关联、告警及分类等功能，此外，态势感知层要按照安全事件的紧急与重要程度来划分优先级和制定对应响应决策，以提供及时有效的应急响应与修复建议。态势可视化层负责将数据处理后的结果以可视化的方式展现给用户，以帮助用户清晰地了解与掌握网络的安全态势，如可视化评估预测管理、日志告警台态势、资产可用性态势等，该层需要具备强大的交互性与一定的可视化展示能力，将复杂的攻击过程和安全事件以地图、流程图、表等形式呈现给用户，同时需要提供多种分析与查询的功能[2]。另外，态势可视化层能够灵活地集成其他安全系统，如入侵检测与防御系统、安全信息与事件管理系统等，能够实现数据共享，从而协同完成工作，达到高效信息安全防护的目的。

4 信息安全态势感知系统组成结构

4.1 管理门户

感知系统的管理门户负责管理与监控各个方面，具有以下核心功能：①态势仪表盘：负责呈现网络安全的关键指标与总体情况，多以图表、图形的方式来向用户呈现网络攻击的安全事件类型、威胁来源以及未来趋势等重要信息，以辅助相关管理人员迅速了解和掌握网络的安全状况。②个人工作台：负责展现用户个性化的工作流程与信息安全任务，每个用户可以在个人工作台中查看自己的通知提醒、待办事项以及工作任务，同时还能够与其他安全相关的工具与资源进行交互。③综合查询视图：可以用来查询与分析网络中的安全事件，其支持多种过滤器与查询条件，能够帮助用户快速追踪与定位特定的安全事件，同时生成对应的统计数据与报告。④任务执行情况：用来追踪、监控与管理系统的各操作与任务的执行情况，用户在任务执行情况中能够自行查看任务的状态、进度等信息，同时可以对任务进行管理与调度。⑤系统管理功能：负责配置与管理系统的各项参数与组件，用户通过系统管理功能，能够自行设置通知与告警、管理用户的角色与权限、配置系统设置以及备份系统等操作[3]。

4.2 知识库

知识库作为态势感知系统的重要组成部分，负责存储与管理告警、事件、漏洞与威胁等与安全有关的信息，其主要包括手机病毒库、关联分析库、事件特征库以及僵木蠕库等。手机病毒库负责管理与存储手机病毒相关的信息，以帮助用户很好地了解手机病毒的威胁以及能够采取的应对措施；关联分析库提供很多能够直接使用的内置关联规则，以帮助用户有效应对更复杂的威胁与网络环境；事件特征库详细记录了各种事件与威胁的严重程度、影响、特征以及处理建议，可以帮助用户及时理解与应对不同类型的安全事件与威胁；僵木蠕库主要包括蠕虫、木马及僵尸网络等常见的网络安全威胁以及相应的应对措施等[4]。知识库在态势感知系统中起着至关重要的作用，实时识别与处理各种网络安全威胁，同时还能够及时更新与维护各种信息，大幅提高网络信息的安全性。

4.3 任务调度管理

任务调度管理是指制定任务计划、配置与下发任务并执行，而后完成自动化调度的过程。其包括以下几个步骤：①任务生成。任务有两种生成方式，分别是手动创建和自动生成，手动创建是指用户根据实际需要自己创建任务；而自动生成是指系统依照网络状态与安全策略自动生成任务的过程。②任务配置。任务生成后需要根据实际需要与安全策略进行一系列配置，如配置任务类型、执行周期、执行时间等内容。③任务下发。任务下发是指将任务通过本地存储或

网络传输等方式来下发给执行机构的过程。④任务执行。执行机构接收到任务后按照配置信息和任务类型来执行任务，同时需要对任务的执行情况进行实时监控，以保证任务能够如期完成。⑤任务核查。任务核查用于核查任务的执行情况，如核查任务的异常情况、完成情况及执行结果等，以保证任务执行的准确性与有效性。

4.4 策略管理

策略管理包含指标管理与安全策略管理两部分内容，其中，指标管理用于管理与维护系统的运行状态与性能的相关指标，主要内容是定义、采集、存储与分析指标，定义指标时需要结合系统的需求与特点来选择合适的参数与指标类型；采集与存储指标时需要做好存储与备份的工作以保证数据的完整性与准确性；分析指标时需要深入挖掘和分析数据，在此基础上改进和优化系统性能。而安全策略管理用来管理与维护安全相关的指令、规则与策略，主要内容是制定、实施、监控与更新安全策略，制定安全策略时需要结合安全需求，综合考虑系统面临的风险与威胁来采取有效的应对措施；实施与监控策略过程通过实时监控来保证策略的有效执行，从而第一时间发现并修复各类安全问题。

4.5 关联分析

关联分析是一种综合利用数据挖掘、统计分析等技术来深入分析安全事件检测数据和网络数据的安全分析方法，其综合运用各种技术与工具，如聚类分析、网络流量分析、因果关系分析、网络安全扫描器、入侵检测系统等，全面深入分析全部安全事件信息，从而及时发现网络中潜在的安全风险，同时为安全策略的制定提供数据依据。

5 系统测试

5.1 测试准备

为验证论文设计的安全态势感知系统的实际应用性能，搭建系统测试平台，并将其与传统态势感知系统进行对比，通过比对两个系统的响应延时来分析该系统的性能，与此同时，结合实际情况，根据系统测试需求，选择 KDD99 数据集作为此次的测试数据集。KDD99 数据集作为一个常用的网络入侵数据集，包括恶意代码、拒绝服务、探测等各类网络入侵事件。

5.2 测试结果与讨论

实际测试时，测试了不同用户数量的情况下，论文设计的安全态势感知系统与传统态势感知系统的响应延时，具体的测试结果见表 1。

表 1 测试结果

用户数量	系统响应延时 /s	
	设计系统	传统系统
10	0.013	2.556
20	0.046	3.352
30	0.018	4.54
40	0.043	5.266
50	0.034	6.185
60	0.048	6.852
70	0.012	7.246
80	0.053	7.826
90	0.047	8.385
100	0.041	9.985

经测试表明，相较于传统态势感知系统，论文设计的安全态势感知系统在不同用户规模下的响应延时更低，且随着用户数量的不断增加，该安全态势感知系统能够保持较稳定的响应延时，证明该系统具有良好的性能，满足安全态势感知对及时性的要求，具有较高的应用价值。

6 结语

综上所述，论文设计的安全态势感知系统能够满足安全态势感知对及时性的要求，能够保持较稳定的低响应延时，具有较好的性能和较高的实际应用价值。未来，将持续研究与探索人工智能技术，不断完善和优化安全态势感知系统，以使其能够更精准、及时预测网络安全威胁与攻击，实现更智能的自动化，同时提供更灵活的定制化服务，以更好地预测和应对网络中的信息安全威胁与挑战。

参考文献

[1] 徐波.人工智能在电力企业网络安全态势感知中的应用[J].网络安全和信息化,2023(6):52-54.

[2] 李景奇,夏方坤,张伟建,等.水利工控系统网络安全态势感知平台设计与应用[C]//2022(第十届)中国水利信息化技术论坛论文集,2022.

[3] 姚晓飞.工业互联网安全态势感知系统设计与实现[D].北京:中国科学院大学(中国科学院沈阳计算技术研究所),2022.

[4] 张颢芳.基于LSTM-DT模型的网络安全态势感知研究[D].哈尔滨:黑龙江大学,2022.