基于威胁情报的网络安全态势评估方法研究

李学民[1] 顾丽旺[2] 宫克[3]

1. 山东省大数据中心 济南 250011；
2. 山东省市场监管监测中心 济南 250014；
3. 山东省网络安全与信息化技术中心 济南 250011

开放科学（资源服务）标识码（OSID）

摘要：[目的 / 意义] 面对复杂多变的国内外网络安全威胁态势，传统的网络安全技术已经难以发现、评估安全状况，加强威胁情报技术的应用，提升网络安全态势评估的能力已成为网络安全态势评估领域的重要环节。[方法 / 过程] 利用网络安全态势评估方法估算隐患和威胁的影响范围与严重程度，发现网络安全隐患和威胁，掌握当前网络安全情报状况。将威胁情报应用到网络安全态势感知，从威胁态势、脆弱性态势和资产运行态势三个方面入手，构建网络安全态势评估指标体系。以网络安全态势评估指标为导向，构建层次化的网络安全态势评估方法。[结果 / 结论] 通过威胁情报能力的加入，网络安全检测能力得到提升，网络安全态势评估指标更加客观及准确，便于网络安全管理人员对网络安全整体管理做出更科学合理的决策。

关键词：网络安全态势感知；态势评估；网络威胁情报；网络安全指标体系

中图分类号：TP393.08 G35

Research on Network Security Situation Assessment Methods Based on Cyber Threat Intelligence

LI Xuemin[1] GU Liwang[2] GONG Ke[3]

1. Shandong Big Data Centre, Jinan 250011, China;
2. Shandong Provincial Market Supervision and Monitoring Center, Jinan 250014, China;
3. Shandong Network Security and Information Technology Centre, Jinan 250011, China

Abstract: [Objective/Significance] In the face of complex and ever-changing domestic and international cybersecurity threat situations, traditional cybersecurity technologies have become difficult to detect and evaluate security conditions. Strengthening the application of threat intelligence technology and enhancing the ability of cybersecurity situation assessment has become an important link in the field of cybersecurity situation assessment. [Methods/Processes] Using network security situation assessment

作者简介 李学民（1979-），本科，高级工程师，主要研究方向为数字政府、新型智慧城市、网络信息安全等；顾丽旺（1976-），硕士，高级工程师，主要研究方向为政务信息系统安全防护及安全态势监测、密码及区块链技术的政务应用等；宫克（1977-），通讯作者，本科，正高级工程师，主要研究方向为威胁情报、网络信息安全、数字政府建设等，E-mail：gongke@shandong.cn。

引用格式 李学民，顾丽旺，宫克 . 基于威胁情报的网络安全态势评估方法研究 [J]. 情报工程，2023, 9(4): 3-13.

doi:10.3772/j.issn.2095-915x.2023.04.001

methods to estimate the scope and severity of the impact of hidden dangers and threats, identify network security hidden dangers and threats, and grasp the current state of network security intelligence. Applying threat intelligence to network security situation assesment, starting from three aspects: threat situation, vulnerability situation, and asset operation situation, constructs a network security situational evaluation index system. Build a hierarchical network security situation assessment method guided by network security situation assessment indicators. [Results/Conclusions] By incorporating threat intelligence capabilities, network security detection capabilities have been improved, and network security situation assessment indicators have become more objective and accurate, making it easier for network security managers to make more scientific and reasonable decisions on the overall management of network security.

Keywords: Network Security Situation Awareness; Situation Assessment; Cyber Threat Intelligence; Indicator System of Network Security

引言

随着我国网络综合治理体系建设加快推动，强化技术管网治网能力已成为重中之重。为增强自身风险防范能力，我国将网络空间安全治理上升到国家战略层面，进行一系列政策布局，开启我国网络安全大合规时代[1]。当前网络结构日益复杂，网络攻击技术和手段层出不穷，传统的安全威胁检测技术已不足以应对如此复杂多变的网络环境。网络安全态势感知（NSSA, Network Security Situation Awareness）能够动态地提取和分析网络系统数据，理解网络攻击意图，主动采取防御措施，已经成为网络安全技术的一个研究热点。将态势感知理论和方法应用到网络安全领域，针对能够引起网络环境变化的大量安全数据，采用相关的分析方法，对网络安全状况进行分析与理解、评估与预测、应急处置以及判断发展趋势的处理过程[2]。网络威胁情报（CTI, Cyber Threat Intelligence）描述了攻击行为，提供了网络攻击的上下文数据（图 1），能够指导网络攻击和和防御，为网络安全态势感知模型的发展提供了新的思路[3]。

网络威胁情报是关于 IT、信息资产面临现有或酝酿中的威胁的证据性知识，包括可实施上下文、机制、标示、含义和能够执行的建议，这些知识可以为威胁的响应、处理决策提供技术支持。

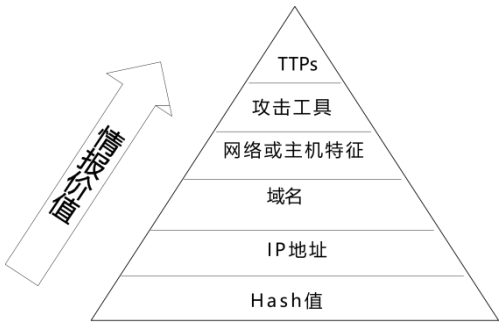

图 1 威胁情报类型及价值

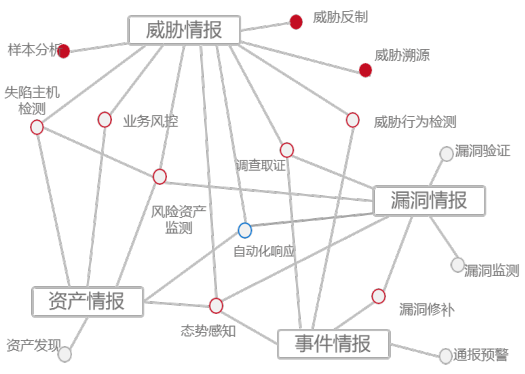

图 2 威胁情报在网络安全态势感知的应用

基于威胁情报收集和分析网络系统中的代表性数据，发现攻击行为的重要信息与攻击特征，可以预判潜在的威胁，为安全事件的响应、防御策略的制定提供高效的处理决策（图 2）。

本文探讨了网络安全态势感知范畴内的威胁情报，提出一组基于威胁情报的网络安全态势评估指标，基于评估指标研究了一种层次化网络安全态势的评估方法。

1 研究现状

Tim Bass 于 1999 年提出网络态势感知概念 [4]，次年将该技术应用于多个网络入侵检测系统检测结果的数据融合分析。在态势感知方面，目前国外的态势感知模型主要有 Endsley 模型、Bass 模型、JDL 模型、OODA 模型等。Endsley 模型由 M. R. Endsley 提出，包括态势要素提取、态势理解和态势预测三个部分 [5]，是当前最主流的网络安全态势感知模型。Bass 模型是由 Tim Bass 提出，模型主要包含了数据感知层、态势评估层、知识转化层，并有独立的查询选择和反馈循环模块，可以协调各层之间的协作并评估系统的整体运行情况 [6-8]。JDL 模型 (Joint Directors of Laboratories) 是以数据融合为核心的态势感知模型 [9]。OODA[10] 模型来源于信息战对抗时遵循的“观察（Observe）、调整（Orient）、决策（Decide）以及行动（Act）”循环过程（图 3）。

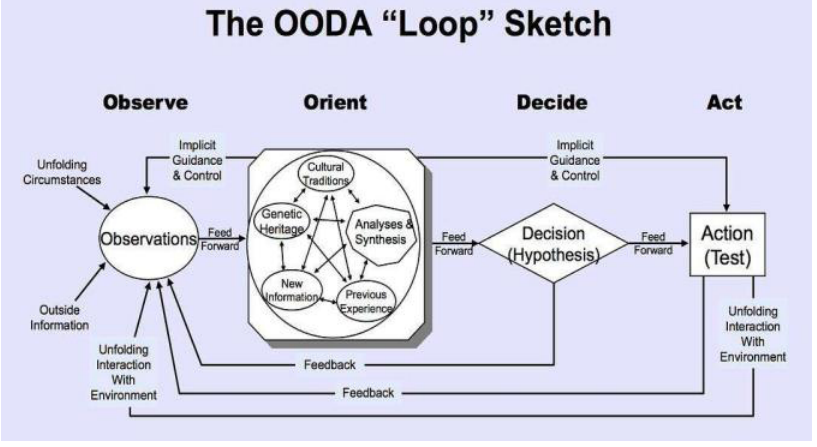

图 3　OODA 模型

丁华东等 [11] 提出了基于贝叶斯方法的网络安全态势感知混合模型，并给出态势等级评定。王一琁 [12] 提出了一个基于知识图谱的网络安全态势感知模型，给出了一种基于资产的网络安全知识图谱的构建方案，并在建成网络安全知识图谱的基础上，针对网络安全态势感知领域的两个经典问题——网络攻击场景发现和态势理解问题，给出了解决方案。

威胁情报记录了既往网络安全事件的典型特征，能够为网络安全策略决策提供有力的辅助，威胁情报共享系统已经越来越受到广泛的重视。威胁情报包含网络环境中设备、网络、系统、应用等产生的安全数据与事件，提供了过往攻击行为的上下文数据 [13]。目前提供威胁

doi:10.3772/j.issn.2095-915x.2023.04.001

情报服务的实体主要有戴尔全球威胁情报 (Dell Global Threat Intelligence)，其能够提供漏洞、威胁和咨询三种基于订阅的数据服务；赛门铁克构建的全球情报网络 (GIN)；国内的 360 公司建设了全国首个企业威胁情报中心。将威胁情报应用于网络入侵检测的研究还处于起始阶段，相关研究成果还很少。文献 [14] 提出的 CyTIME 框架探讨了从威胁情报共享数据中心获取和融合威胁情报的方法。文献 [15] 给出了一种基于深度学习方法，由威胁情报自动生成入侵检测规则的方法，能够较好地发现恶意代码攻击。

2 基于威胁情报的网络安全态势评估指标

网络系统从业务逻辑关系上可以分为设备、网络、系统与应用三个层次。网络安全态势评估需要针对三个不同层次主体安全状况进行评价和估测。评估内容包括网络系统中发生的安全事件、系统漏洞情况、系统冗余情况、系统响应情况等，归纳起来可以划分为威胁态势、自身的脆弱性态势以及网络系统的整体资产运行态势三个主要方面（图 4）。

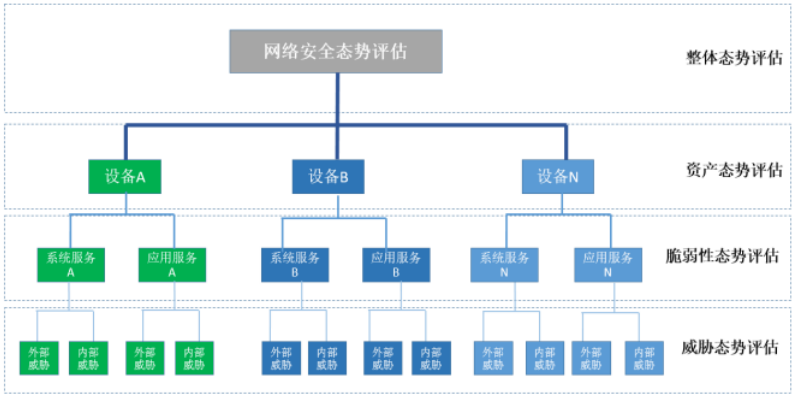

图 4　网络安全态势评估层次分析

2.1 威胁态势

威胁态势评估是指通过系统、网络、资产等发生的内部和外部安全事件评价，评估可能对网络系统产生的安全影响。内部安全事件又可称为内部攻击，包括人员对系统、应用或数据的误操作、越权使用、非法访问等。外部安全事件又称为外部攻击，是指系统、应用、网络、资产等遭受源自被评估系统以外的攻击活动。外部攻击包括针对网络或应用服务等的 DDoS 攻击；针对系统或应用的恶意代码攻击；针对系统或应用的入侵活动以及网络欺诈等其他攻击活动。因此在选择威胁方面指标时，主要考虑网络系统内外的网络安全事件，可以根据攻击特征和攻击前后目标资产和网络的变化对攻击进行分类，并针对每种类型的攻击提取威胁评估指标。可利用的威胁情报来自设备日志、网络告警记录、网络流量变化以及其他相关情报。评估指标应包括告警的数量、安全事件频率、网络流量变化、网络带宽变化率等，从而可以通过历史和实时的安全事件情况开展评估工作，

使管理者掌握人为的内部和外部因素对网络安全施加的影响情况。

2.2 脆弱性态势

脆弱性态势包括资产脆弱性和网络脆弱性。通过对网络系统中资产、网络等自身存在的漏洞或弱点的评价，可以评估网络系统自身的脆弱性态势。

资产脆弱性包括设备和系统及应用软件的软件方面脆弱性和物理方面脆弱性。软件方面的脆弱性是指系统和应用软件等存在的漏洞情况，这些系统漏洞是可被恶意利用的弱点，是系统安全的潜在风险。资产脆弱性评估需要针对资产漏洞的整体情况、各危害级别漏洞的分布情况，补丁的安装情况、端口开放情况等，对资产软件方面的脆弱性进行评估。物理方面脆弱性是指资产物理设施自身可靠性，例如能源保障情况、电气性能情况、平均故障率等。网络脆弱性是指网络拓扑结构上存在的缺陷，网络脆弱性评估从复杂网络理论出发，讨论网络节点、网络链路等形成的结构特性，例如节点度分布、中心性、核数、介数等，从而评估网络拓扑结构存在的弱点对网络服务性能影响等问题。

脆弱性态势的威胁情报包括系统漏洞情况、系统配置、系统灾备、网络结构等。评估指标包括端口开放数量、漏洞数量、漏洞级别比率、设备灾备比率、网络灾备比率、网络结构脆弱性。

2.3 资产运行态势

资产运行态势包括设备运行态势、系统软件运行态势、应用软件运行态势和网络运行态势，描述了网络系统整体的运转情况和持续服务的能力。设备运行态势是对所有物理设备的运行状态和服务能力的持续跟踪和监测，包括CPU 占用率、内存使用率、网络流量、开放端口、平均故障率、平均连接数等，描述了网络整体运行的情况。系统软件运行态势是针对软件的版本情况、系统的平均响应时间、平均故障率等进行监测；应用软件运行态势是针对软件服务能力的评估，包括平均连接数、平均服务时间、平均响应时间、平均故障率等。这两者代表了系统和应用软件持续服务的能力和运行态势。网络运行态势描述了网络服务的运行态势，包括拓扑结构的变化监测、网络流量变化监测、网络带宽变化监测、网络延迟情况监测等。威胁情报的获取需要使用网络系统中的各种传感器，评估指标应该包括资源利用率、系统连接数、系统响应时间、系统故障率、网络带宽变化等。

2.4 网络安全态势评估指标

基于以上论述，从威胁态势、自身的脆弱性态势以及网络系统的整体资产运行态势多个维度，针对网络系统的设备、网络、系统与应用三个层次，提取了以下网络安全态势评估指标，如表 1 所示。

在威胁态势的评估指标方面，需要分别研究不同类别的网络攻击，然后从中提取具有共性和可操作的指标。在脆弱性态势的评估指标方面，主要研究资产脆弱性和网络脆弱性两个方面对网络安全脆弱性的评估要素，提取脆弱性评估指标。在资产维度的评估指标方面，主要从评估网络系统整体的正常运转和持续服务的能力角度开展，研究网络系统的资产运行情况、服务能力状态等方面的评估要素（图 5）。

doi:10.3772/j.issn.2095-915x.2023.04.001

表 1　网络安全态势评估指标

一级指标	二级指标	三级指标
威胁态势	威胁性	告警数量 网络流量 网络流量增长率 网络带宽使用率 安全事件历史发生频率 网络服务中断率 应用服务中断率 设备服务中断率 服务系统中断率 攻击源数量 攻击源分布 服务恢复率
脆弱性态势	脆弱性	漏洞数量 漏洞级别比率 端口开放数 安全设备数量 灾备率 网络结构脆弱性
资产运行态势	功能性	CPU利用率 内存利用率 磁盘利用率 带宽利用率 设备故障率
	服务性	网络延迟情况 网络连接数量 网络连接变化率 系统服务平均响应时间 应用服务平均响应时间 系统服务中断时间 应用服务中断时间

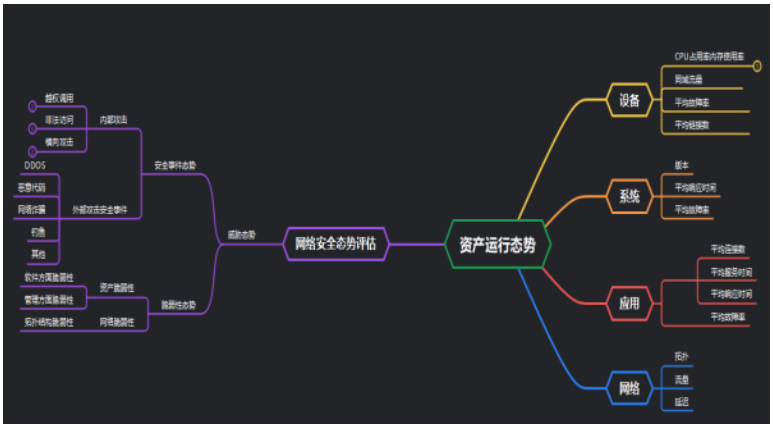

图 5　网络安全态势评估指标示意

3 层次化网络安全态势评估

通过对上述的评估指标进行统计计算，可以从设备、网络、系统与应用三个层面估算网络系统面临的威胁态势、自身脆弱性态势以及网络资产运行态势，从而得到整个网络系统的安全态势。评估模式如图 1 所示。

时刻 t 系统或应用 S_j 的威胁态势指数为：

$$R_{S_j}(t)=\sum_{j=1}^{n}D_j(t)$$

其中，$R_{Sj}(t)$ 为 t 时刻系统或应用 S_j 的威胁态势指数；$D_j(t)$ 为 t 时刻某类安全事件的威胁态势评估值；n 为适用于系统或应用 S_j 的威胁态势指标数。

在时刻 t 设备 H_k 的脆弱性态势指数为：

$$R_{H_k}(t)=\sum_{j=1}^{m}V_iC_i(t)$$

其中，$R_{Hk}(t)$ 为 t 时刻设备 H_k 的脆弱性安全态势指数；$C_i(t)$ 为脆弱性态势指数；V_i 为服务 i 在设备 H_k 漏洞与网络脆弱性所占的权重；m 为针对设备 H_k 漏洞与网络脆弱性数量。

在时刻 t 资产运行态势指数为：

$$R_{L_k}(t)=\sum_{k=1}^{n}W_kU_k(t)$$

其中，$R_{Lk}(t)$ 为 t 时刻网络资产 L_k 的运行态势指数；$U_k(t)$ 为运行态势指数；W_k 为指标的重要性权重；n 为被评估指标的数量。

然后，可以计算网络系统的 t 时刻威胁态势指数 $RS(t)$：

$$RS(t)=\sum_{j=1}^{n}R_{s_j}u_j$$

u_j 为系统或应用 S_j 的重要性权重。类似的可以定义 t 时刻网络系统的脆弱性态势指数和资产运行态势指数 $RH(t)$、$RL(t)$。然后可以得到 t 时刻整体性安全态势指数为：

$$S=(RS(t),RH(t),RL(t))^T*(w_s,w_H,w_L)$$

S 为整体网络安全态势评估指数；w_S、w_H、w_L 分别为威胁态势、脆弱性态势以及资产运行态势指标的重要性权重。通过整体性态势指数刻画网络系统整体的安全态势情况，从而得到网络安全态势评估的结果。

4 实验验证

本文通过在实验室构建环境，开展网络安全态势评估指标研究验证，其中检测条件分别为加入威胁情报检测引擎进行检测及不加入威胁情报检测引擎。

4.1 实验环境

本次验证环境采用实验室虚拟靶机环境，通过在模拟靶机系统随机仿真真实政务业务系统，并通过打流设备模拟真实业务系统间的网络流量交互，建立模拟真实业务系统的试验环境。

在模拟的业务系统的虚拟核心交换处进行流量镜像，分别将流量镜像至启用威胁情报检测引擎的检测设备及不启用威胁情报检测引擎的检测设备。同时对相同的流量内容进行检测分析。检测拓扑如图 6 所示。

doi:10.3772/j.issn.2095-915x.2023.04.001

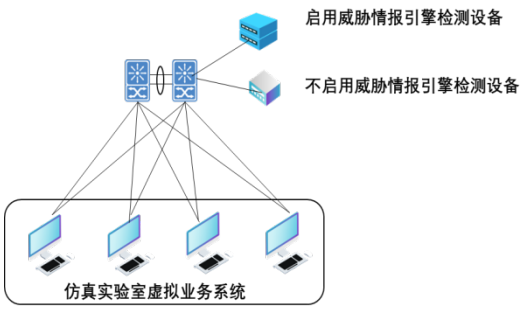

图 6 实验验证环境

4.2 实验现象

实验用的检测设备内置威胁检测情报引擎。并内置威胁态势评估算法，可对整个业务系统的威胁态势、脆弱性态势、资产运行态势分别进行评估，并记录所得到的指标结果。

实验过程中，基于实际实验环境分析，指数 n，m 设定为 5，不启用威胁情报，在固定时间抓取各类数据为：

表 2 不启用威胁情报各项数据

类别	数值
$D_j(t)$	0.05
$R_{S_j}(t)$	0.25
V_i	0.4
$C_i(t)$	0.6
$R_{Hk}(t)$	0.8
W_k	1.5
$U_k(t)$	42
$R_{Lk}(t)$	37
u_j	1
S	54.76

启用威胁情报，在同样固定时间抓取各类数据为：

表 3 启用威胁情报各项数据

类别	数值
$D_j(t)$	0.12
$R_{S_j}(t)$	0.6
V_i	0.6
$C_i(t)$	0.4
$R_{Hk}(t)$	1.8
W_k	1.5
$U_k(t)$	32
$R_{Lk}(t)$	52
u_j	1
S	17.62

表 2、表 3 最终得到的整体网络安全态势评估指数评分越低代表发现的安全事件越多、漏洞脆弱性越强，网络安全风险越高。整体网络安全态势评估指数大概呈现 3 倍的数值范围浮动，意味着启用威胁情报进行安全检查，检测结果将与威胁情报命中数量能力成正比，也证明了威胁情报的参与，提升了整网安全态势评估的能力。

各类细节指标如表 4、表 5 所示。

未加入威胁情报检测引擎，检测 1G 流量产生的安全告警有 1125 条，检测到漏洞数量为 2120 个，其中漏洞均为中低危漏洞，检测到端口开放数 1205。

加入威胁情报检测引擎，检测 1G 流量产生的安全告警有 3367 条，检测到漏洞数量为 3342 个，其中漏洞均为中高危漏洞，检测到端口开放数 1541。

通过调整威胁情报中的威胁、脆弱性、资产三类情报数量，查看整体网络安全态势评估指数情况。

表 4　不启用威胁检测情报引擎网络安全态势评估各项指标结果

一级指标	二级指标	三级指标	数值
威胁态势	威胁性	告警数量	1125
		网络流量	1Gbps
		网络流量增长率	20Mbps
		网络带宽使用率	60%
		安全事件历史发生频率	减少
		网络服务中断率	10%
		应用服务中断率	0%
		设备服务中断率	0%
		服务系统中断率	0%
		攻击源数量	109
		攻击源分布	13
		服务恢复率	90%
脆弱性态势	脆弱性	漏洞数量	2120
		漏洞级别比率	中低危漏洞比例高
		端口开放数	1205
		安全设备数量	5w
		灾备率	100%
		网络结构脆弱性	中
资产运行态势	功能性	CPU利用率	80%
		内存利用率	90%
		磁盘利用率	0%
		带宽利用率	60%
		设备故障率	10%
	服务性	网络延迟情况	低延时
		网络连接数量	1w
		网络连接变化率	10%
		系统服务平均响应时间	10s
		应用服务平均响应时间	10s
		系统服务中断时间	10s
		应用服务中断时间	10s

doi:10.3772/j.issn.2095-915x.2023.04.001

表 5　启用威胁检测情报引擎网络安全态势评估各项指标结果

一级指标	二级指标	三级指标	数值
威胁态势	威胁性	告警数量	3367
		网络流量	1Gbps
		网络流量增长率	20Mbps
		网络带宽使用率	60%
		安全事件历史发生频率	增加
		网络服务中断率	10%
		应用服务中断率	0%
		设备服务中断率	0%
		服务系统中断率	0%
		攻击源数量	328
		攻击源分布	47
		服务恢复率	90%
脆弱性态势	脆弱性	漏洞数量	3342
		漏洞级别比率	中高危漏洞比例高
		端口开放数	1541
		安全设备数量	5w
		灾备率	100%
		网络结构脆弱性	中
资产运行态势	功能性	CPU利用率	80%
		内存利用率	90%
		磁盘利用率	0%
		带宽利用率	60%
		设备故障率	10%
	服务性	网络延迟情况	低延时
		网络连接数量	1w
		网络连接变化率	10%
		系统服务平均响应时间	10s
		应用服务平均响应时间	10s
		系统服务中断时间	10s
		应用服务中断时间	10s

4.3　实验结论

本次实验结果表明，威胁情报的加入给安全威胁检测、安全漏洞检测的能力提升约三倍。基本符合模型计算预期，应用基于威胁情报的网络安全态势评估指标所开展的层次化网络安全态势评估方法极大地提升了网络安全检测的能力和水平，对网络安全态势评估能力提升的作用效果显著。

5　结束语

网络安全态势评估是一项复杂而艰巨的工作，涉及场景繁复多样，使用的数据类型多样、规模巨大，尤其是大数据环境下更是增加了评估的复杂性。网络安全态势评估作为网络安全态势感知中的重要环节，具有非常重要的意义和作用。本文研究了基于威胁情报的网络安全态势评估方法，根据威胁情报，从威胁态势、脆弱性态势和资产运行态势三个方面着手建立评估指标，并依据这些指标计算当前网络的安全状态，从感知效率、感知实用性、感知客观性分析了网络安全态势情报指标的作用，选取自上而下的模型方法综合评估了威胁态势、自身的脆弱性态势及网络系统的整体资产运行态势，结合科学评估方法进行了多维量化研究。研究结果表明，通过基于威胁情报的层次化网络安全态势评估情报指标，常态化开展网络安全态势评估情报指标评估，科学评估隐患和威胁的影响范围与严重程度，掌握当前网络安全情报和安全状况，面对网络安全威胁统一监控、准确应对、快速反应，强化技术管网治网能力，为加快推进我国网络综合治理工作提供有力技术支撑。

参 考 文 献

[1]　张红斌，尹彦，赵冬梅，等．基于威胁情报的网络安全态势感知模型 [J]. 通信学报，2021, 42(6): 182-194.

[2] 龚正虎 , 卓莹 . 网络态势感知研究 [J]. 软件学报 , 2010, 21(7):1605-1619.

[3] 龚俭 , 臧小东 , 苏琪 , 等 . 网络安全态势感知综述 [J]. 软件学报 , 2017, 28(4): 1010-1026.

[4] BASS T, GRUBER D. A glimpse into the future of ID[J]. The Magazine of USENIX & SAGE, 1999, 24(3): 40-49.

[5] ENDSLEY M R. The divergence of objective and subjective situation awareness: A meta-analysis [J]. Journal of Cognitive Engineering and Decision Making, 2020, 14(1): 34-53.

[6] BASS T. Multi-sensor data fusion for next generation distributed intrusion detection systems[C]. Proceedings of IRIS National Symposium on Sensor and Data Fusion, 1999:24-27.

[7] BASS T. Intrusion Detection Systems and Multisensor Data Fusion: Creating Cyberspace Situational Awareness[J]. Communications of the ACM, 2000, 43(4):99-105.

[8] BASS T. Cyberspace Situation Graphs-A Brief Overview (Presentation) [EB/OL]. [2016-9-26]. www.thecepblog.com.

[9] SCHREIBER-EHLE S, KOCH W. The JDL model of data fusion applied to cyber-defence—a review paper[C]. 2012 Workshop on Sensor Data Fusion: Trends, Solutions, Applications (SDF). IEEE, 2012: 116-119.

[10] LENDERS V, TANNER A, BLARER A. Gaining an edge in cyberspace with advanced situational awareness[J]. Security & Privacy IEEE, 2015, 13(2):65-74.

[11] 丁华东 , 许华虎 , 段然 , 等 . 基于贝叶斯方法的网络安全态势感知模型 [J]. 计算机工程 , 2020, 46(6):130-135.

[12] 王一琁 . 基于知识图谱的网络安全态势感知技术研究与实现 [D]. 成都 : 电子科技大学 , 2020.

[13] 赵宁 , 李蕾 , 刘青春 , 等 . 基于网络开源情报的威胁情报分析与管理 [J]. 情报杂志 , 2021, 40(11):8.

[14] KIM E, KIM K, SHIN D, et al. CyTIME: Cyber threat intelligence management framework for automatically generating security rules[C]. Proceedings of the 13th International Conference on Future Internet Technologies, 2018: 1-5.

[15] 刘亮 , 赵倩崇 , 郑荣锋 , 等 . 基于威胁情报的自动生成入侵检测规则方法 [J]. 计算机工程与设计 , 2022, 43(1): 1-8.