基于开源信息平台的威胁情报挖掘综述

崔 琳[1], 杨黎斌[1], 何清林[2], 王梦涵[1], 马建峰[3]

[1]西北工业大学 网络空间安全学院 西安 中国 710129
[2]国家互联网应急中心 北京 中国 100029
[3]西安电子科技大学 网络与信息安全学院 西安 中国 710071

摘要 网络空间新生威胁日趋复杂多变, 传统安全防御手段已经捉肘见襟。网络安全威胁情报作为直接或潜在安全威胁的外部信息资源, 可帮助安全人员快速甄别恶意威胁攻击并及时作出响应防御。开源威胁情报挖掘技术可从多方开源情报中获取高质量情报, 极大弥补了传统威胁情报挖掘信息量单薄等不足。美国及欧洲是最早在政府层面开展开源情报挖掘技术研究的国家和地区, 并将其作为政府的常规情报搜集手段。近年我国也在广泛采集整理网络开源威胁信息, 并拓展开源威胁情报的应用。本文深入分析了近 6 年来开源威胁情报挖掘的一百多篇相关文献, 系统梳理了威胁情报挖掘相关文献的技术理论以及在网络安全检测中的应用场景, 归纳总结出了开源威胁情报挖掘的一般流程框架模型, 并针对开源威胁情报采集与识别提取, 开源威胁情报融合评价以及开源威胁情报关联应用三个关键场景进行了分析和论述, 系统评述了这三部分研究工作中的细分热点方向, 并从技术应用场景, 所使用的技术, 性能评估以及优缺点评价对各解决方案做了系统优劣势分析; 最后分析总结了当前我国开源威胁情报挖掘中尚待解决的共性问题, 并指出了未来的研究趋势与下一步研究方向。本文期望通过研究和分析已有的开源威胁情报研究概况, 推进我国开源威胁情报挖掘分析工作的发展, 提升国家网络安全的整体防御能力。

关键词 开源威胁情报; 识别提取; 融合评价; 关联分析
中图法分类号 TP391.1 DOI 号 10.19363/J.cnki.cn10-1380/tn.2022.01.01

Survey of Cyber Threat Intelligence Mining Based on Open Source Information Platform

CUI Lin[1], YANG Libin[1], HE Qinglin[2], WANG Menghan[1], MA Jianfeng[3]

[1] School of Cyberspace Security, Northwestern Polytechnical University, Xi'an 710129, China
[2] National Internet Emergency Center, Beijing 100029, China
[3] School of Cyber Engineering, Xidian University, Xi'an 710071, China

Abstract Traditional security defense measures are struggling to keep pace with the increasing sophistication of attack tools and methodologies. The emerging of network security threat intelligence is a promising approach for alleviating maliciously attacks, by providing additional information to depict full picture of the fast-evolving cyber threat situation. Open source cyber threat intelligence (OSCTI) mining technology can obtain high-quality intelligence from multiple open source intelligence, which makes up for the deficiency of traditional threat intelligence mining. The United States and Europe make efforts to implement relevant strategies for the sake of established developing OSCTI mining system. Rcentently, China also tends to expand the mining and application of OSCTI by deeming it as a key supplement of cyber security defense system, such as situation awareness platform, next-generation firewall and intrusion detection system. Under such circumstances, we conduct the first comprehensive and systematic survey of OSCTI mining solutions in this paper. We investigate hundreds of literatures on open source threat intelligence mining over the period 2015–2020 in depth, and systematically classify the process of OSCTI mining as three key perspectives on identification and extraction, fusion and evaluation, correlation analysis. We sketch the main idea and highlight the strengths and weaknesses of each solution type, and summarize the similarity and difference among solution types by analyzing technology application scenarios, technologies used, performance evaluation and advantages and disadvantages evaluation, etc. We further analyze the shortcomings of open source threat intelligence mining and application research in China at present, summarize four opportunities and challenges, suggest several potential trends and future directions in open source cyber threat intelligence mining allowing for a deeper and better investigating. We hope that it can provide academic researchers and industrial practitioners with useful and valuable references for combating serious cyber-attack, responding to the increasingly severe network security situation, and therefore securing internet ecosystem.

通讯作者: 杨黎斌, 博士, 副教授, Email: libiny@nwpu.edu.cn。
本课题得到国家自然科学基金(No. 61772429)、国家 242 信息安全专项(No. 2021A017)与陕西省重点研发计划(No. 2020ZDLGY08-01)资助。
收稿日期: 2021-05-21; 修改日期: 2021-08-20; 定稿日期: 2021-11-11

Key words open source cyber threat intelligence; recognition and extraction; fusion and evaluation; correlation analysis

1 引言

随着万物互联的时代到来, 互联网由于其固有的多源异构, 泛在开放等特性, 使其在享受“云大物移智”等新型技术便利的同时, 其所面临的新生网络威胁也日趋复杂多变, 各种新型安全攻击事件频发。尤其是在大国博弈的背景下, “震网”、“火焰”、“毒区”等高级可持续威胁(Advanced Persistent Threat, APT)攻击陆续出现, 当前网络空间的安全威胁问题日益严峻。根据 CNCERT 的研究, 近年来我国逐渐成为各类网络攻击的重灾区, 而其中以 APT 和 DDoS 为代表的新型攻击所占的比重越来越大。表 1 列出了近年来的一些新型网络安全威胁类型。

表 1 新生威胁及其特点

Table 1 Emerging threats and their characteristics

类型	描述	特点	意图
APT	攻击者通过构造一种长时间, 分阶段的复杂网络攻击, 尝试获得网络系统的访问权, 并在很长一段时间内保持不被发现[1]。	多向和多阶段威胁	窃取数据
多态威胁	木马或病毒通过加密或压缩等方式实现自我隐藏, 保持对目标的威胁攻击。	通过修改程序特性改变自身形态	网络权限提升
零日威胁	利用尚未公开披露或供应商尚未发现及未修补的漏洞, 对系统和应用程序进行威胁攻击。	利用尚未修复未公开披露的漏洞	使系统失能
复合威胁	联合技术工具和社会工程技术来获得系统特权信息。	句法攻击和语义攻击的结合	获取网络系统主机权限

可以看出, 随着目标场景变化, 恶意攻击者将网络空间攻击的复杂性和影响力提升到前所未有的程度, 其攻击模式、数量与种类层出不穷。这些新型攻击充分利用了 web、电子邮件、应用程序等多种传播方式, 且可在网络系统中相互渗透, 以捕获有价值的数据, 具有常态化、专业化、多矢量、多阶段等特性。由于新型攻击的这些特性, 加之攻击者的先手优势, 这也对现今网络空间的威胁防护提出了新的挑战。传统安全防御方法大多依靠部署于边界或特殊节点的防火墙、入侵检测系统等安全设备, 通过基于启发式和签名等静态检测方法, 将每个攻击向量视为一个单独路径进行分阶段独立检查, 而缺少全局视角, 难以应对攻击策划精妙、更新迭代频繁的新型网络威胁攻击。

针对网络空间所面临的新型安全威胁, 一个重要的防护手段是深度挖掘网络威胁的情报信息, 并将其引入至安全检测全周期中, 从而主动发现并防御恶意且极难检测的攻击行为。网络威胁情报(Cyber Threat Intelligence, CTI)挖掘技术通过收集、挖掘、识别实时网络威胁信息并将其转化为威胁情报。一般来说, 威胁情报是指可用于解决威胁或应对危害的知识, 包括威胁来源、攻击意图、攻击手法、攻击目标信息, 具有知识密度大、准确性高、关联性强等特点, 能够为安全分析的各个阶段提供有力的数据支撑, 并可针对多态、复杂的高智能威胁与攻击做出及时响应防御。

根据来源不同, 威胁情报一般可分为内部威胁情报和外部威胁情报, 如图 1 所示, 其中内部威胁情报一般来源于目标系统中的内部安全事件信息, 可通过入侵检测系统(IDS)等安全设备中的相关信息提纯获得。外部来源的威胁情报包括: (1) 商业威胁情报, 即安全厂商以产品形式出售或分享的商业威胁信息; (2) 开源威胁情报(Open Source Threat Intelligence, OSTI), 在公开平台中分享的开源威胁情报。近些年由于网络威胁攻击形式迭代更新频繁, 开源威胁情报突破了其他威胁情报形式来源少, 情报特征受限等不足, 以其快速灵活、性效比高、易于移植等特点, 吸引了政府、业界以及学界的广泛关注, 并作为网络防御的重要资源, 在众多实际情景中得到应用。

美国非常重视威胁情报, 从战略、法律、标准、防御体系、与私营部门的信息共享方面都制定了相对完善的机制[2]。美国也是最早在政府层面开展开源情报挖掘技术研究的国家, 并将其作为政府的常规情报搜集手段。当前美国已建立起了覆盖地方、企业、政府等多个层面的开源威胁情报挖掘体系, 重点着眼于开源威胁情报的挖掘技术研究及深度利用。欧洲网络与信息安全局于 2019 年建立了一个整合各方资源的统一开源威胁情报挖掘共享中心, 强调扩大网络威胁情报的收集范围, 包括来自相关学科的

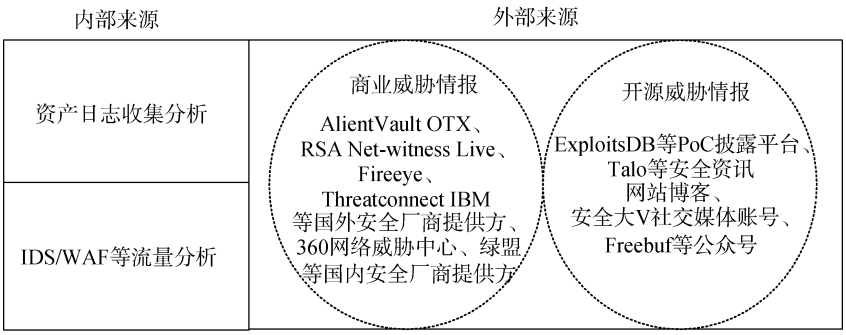

图 1 威胁情报来源

Figure 1 The sources of threat intelligence

事件信息, 并将这些数据的收集、存储和分析标准化。国家应急响应中心 CNCERT 以及国内各大知名安全公司如绿盟, 360 等近年都陆续构建了国内顶尖的开源威胁情报平台, 能够实时采集整理网络开源威胁信息, 并拓展开源威胁情报的应用, 使其成为我国网络安全防御体系的关键组成部分, 贯穿于态势感知平台、下一代防火墙、入侵检测系统等众多的安全产品之中。近年来, 威胁情报市场发展势头良好, 其中威胁情报安全服务提供商的收入也在连年增长。但相较而言, 我国的威胁情报体系发展仍处于起步阶段, 虽然涌现了一批较为出色的威胁情报公司, 并在部分厂商的实际情景中开始落地应用。但总体来看, 其开发及应用主要集中于商业威胁情报, 对于开源威胁情报的关注相对较少, 同时缺乏有效、可靠的威胁情报的挖掘采集、质量评价手段, 其对应基于开源威胁情报的网络安全分析技术也较为落后, 没有形成情报挖掘分析、评价与利用为一体的威胁情报综合服务平台。尽管开源威胁情报已成为安全行业的研究及应用热点, 但仍然存在许多制约开源威胁情报产业链发展的关键问题尚待解决, 包括开源威胁情报挖掘关联、质量评价、落地应用等关键技术的研究。近年来, 学术界结合云计算、大数据等前沿技术对这些关键技术问题进行了深入研究探索。如图 2 所示, 学术研究热度连年上升反映出该领域已持续受到关注, 研究和分析已有的开源威胁情报研究概况, 对于进一步推进我国开源威胁情报挖掘分析工作的发展, 提高国家网络安全的整体防御能力, 具有重要的意义。

本文系统调研分析了近 6 年来主流安全类期刊和会议上关于开源威胁情报挖掘的文献工作, 统计分析了一百多篇文献的技术理论及应用场景, 总结了开源威胁情报挖掘及应用领域当前的研究成果并指出该领域的研究方向, 尝试为我国开源情报挖掘及应用领域进行梳理, 具体来说主要贡献包括 3 个方面:

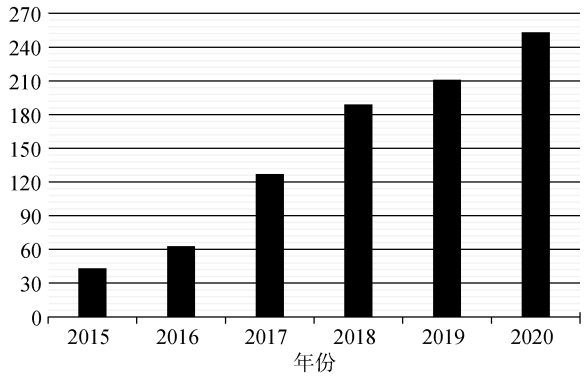

图 2 2015—2020 年基于开源信息平台开源威胁情报挖掘文献分布情况

Figure 2 The distribution of OSCTI mining documents based on open source information platform from 2015 to 2020

(1) 深入分析了开源威胁情报挖掘的一百多篇相关文献, 系统梳理了开源威胁情报挖掘相关文献的技术理论以及在网络安全检测中的应用场景, 归纳总结出了开源威胁情报挖掘的一般流程框架模型;

(2) 首次从开源威胁情报采集与识别提取, 开源威胁情报融合评价和开源威胁情报关联分析等三个方面对开源威胁情报所面临的问题以及对应的研究现状进行了梳理总结, 并从技术应用场景, 所使用的技术及性能评估等方面对相关文献进行了详细解析;

(3) 分析了当前我国开源威胁情报挖掘及应用研究中的不足, 总结了面临的四大机遇与挑战, 并指出了未来的研究趋势与下一步研究方向。

2 开源威胁情报挖掘框架

根据《网络威胁情报权威指南》中给出的定义, 威胁情报是指对企业可能产生潜在或直接危害的信息集合。这些威胁信息经过搜集、分析、整理, 能帮助企业研判面临的威胁并做出正确应对, 以保护企

业的关键资产。从开源情报的直观定义出发, 开源情报在挖掘并应用到关键资产保护时, 其安全应用场景可总结为图 3 所示, 已有绝大部分开源威胁情报挖掘的研究工作都可以纳入到该框架中。

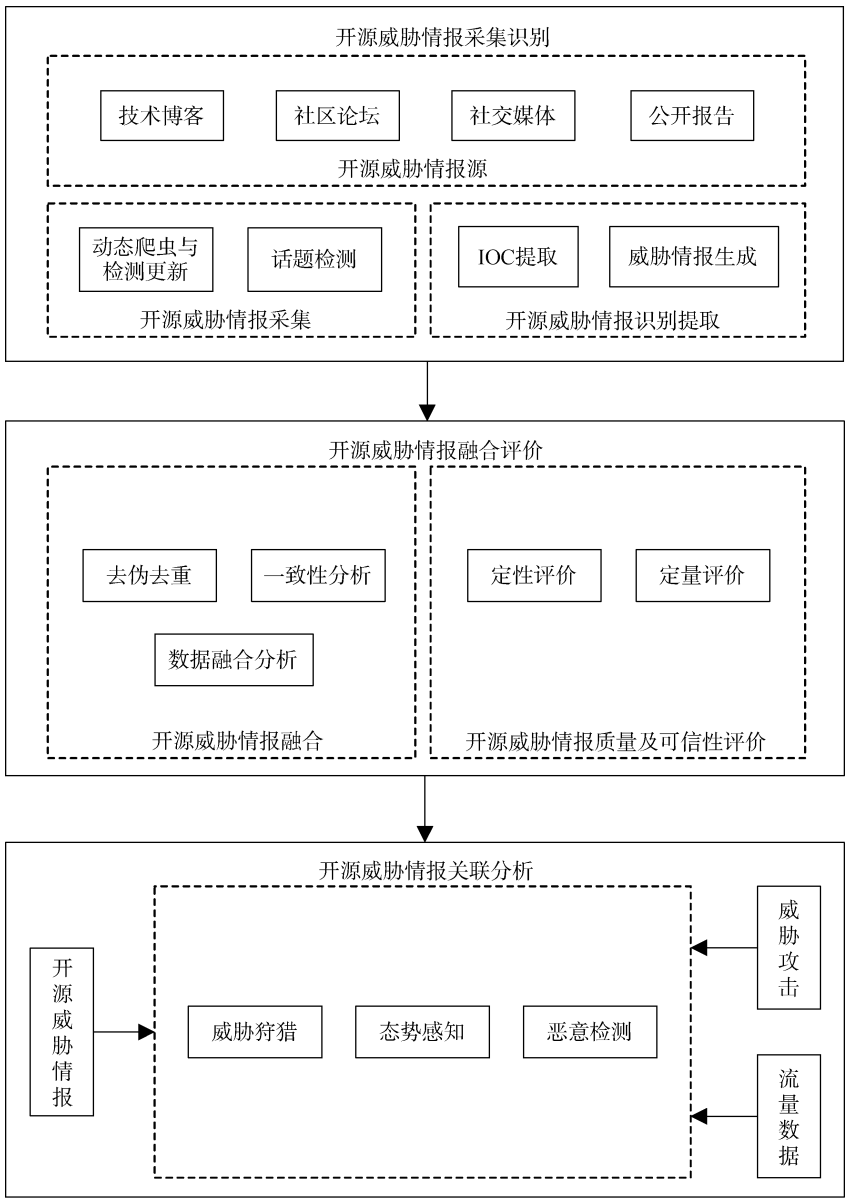

图 3　基于开源信息平台开源威胁情报挖掘框架

Figure 3　OSCTI mining framework based on open source information platform

开源威胁情报挖掘的整体框架自顶向下可归纳为开源威胁情报采集识别、融合评价和关联分析等三大关键研究子方向。其中各子方向功能介绍如下:

(1) 开源威胁情报采集识别

该研究子方向主要针对不同开源情报信息载体, 如技术博客、社区论坛、社交媒体和公开报告等, 利用动态爬虫与检测更新等方法, 获取威胁情报的基础信息; 由于开源信息平台其数据内容通常是文本表示形式, 开源情报信息获取时一般需要通过 IOC(Indicator of Compromise)提取等技术手段, 将其转换成非标准化或 OpenIOC(Open Indicator of Compromise), STIX(Structured Threat Information eXpression)等标准化开源威胁情报格式, 而后分别应用于质量评价阶段和应用检测阶段;

(2) 开源威胁情报融合评价

由于开源威胁情报来源的开放性, 使其挖掘得到的情报信息也具有多源异构性, 对应情报的质量及可信性也参差不齐, 这将阻碍开源威胁情报的存储和共享, 应用于安全场景检测时也可能引发漏报、误报等不可控问题。在实际应用时, 一般需要对多源异构的开源威胁情报信息进行融合评价处理。开源威胁情报融合评价主要是针对多源异构开源威胁情

报基础数据进行整合、萃取和提炼, 并研究建立相关质量评价指标对开源威胁情报的质量及可信性进行评价, 为后续威胁情报和威胁攻击的关联挖掘提供输入线索;

(3) 开源威胁情报关联分析

这部分研究主要针对开源威胁情报的落地应用, 一般是综合运用 Kill-Chain 模型、钻石模型或异质信息网络等模型, 在不同应用场景中结合已有开源威胁情报与实时流量数据, 对威胁情报进行深度关联、碰撞、分析操作, 以发现一些潜在的攻击行为, 推理挖掘揭示出隐含的攻击链条等威胁信息等。以开源威胁情报为应用核心的关联分析研究工作在当前较为热门, 大致可分为网络狩猎、态势感知、恶意检测等三个应用场景, 在后续章节中将详细论述。

以上是开源威胁情报挖掘的一般流程框架模型, 涵盖了开源威胁情报挖掘中较为重要的研究方向, 具有一定的普适性和通用性。通过梳理该流程框架, 可帮助初涉此方向的研究者对开源威胁情报挖掘研究领域做整体把握, 也可辅助细分方向的研究者予以借鉴, 突破固有局限性, 解决现有研究的问题。在接下来论述中, 将按照此框架模型, 依次针对开源威胁情报采集与识别提取, 开源威胁情报融合评价和开源威胁情报关联分析三大研究子方向进行详细论述。

3 开源威胁情报采集与识别提取

传统的威胁情报采集与识别一般具有固定获取途径, 主要依赖从安全厂商过往的网络威胁攻击数据中提炼, 例如包括从企业内部网络、终端部署的检测设备或高交互蜜罐中产生的日志数据, 也有一大部分威胁情报来源于订阅的安全厂商、行业组织收集的威胁数据等。随着网络攻击的数量和复杂度迅速增加[3], 基于传统途径的内部威胁情报收集手段和方式[4-10]难以从根本解决威胁情报来源单一等不足。开源信息平台安全应用[11-17]发展和安全需求催生出的开源威胁情报自动获取和识别技术为解决传统威胁情报的固有弊端提供了行之有效的新路径。从技术方法来看, 现有开源威胁情报采集研究工作主要集中于研究设计自动化爬虫及解析技术, 从安全论坛和博客等平台获得非结构化语义文本数据。本节依据开源情报信息载体的不同, 将其划分为技术博客、社区论坛、社交媒体、公开报告、通用方法等五个开源威胁情报识别提取平台并依此筛选分析代表性的相关研究工作, 接下来, 针对这五个平台中开源威胁情报的识别提取研究工作进行分别阐述。

3.1 开源威胁情报采集

开源威胁情报采集是指从多个不同来源的开源数据选取目标开源信息(如目标博客网站内容)作为输入, 输出可被进一步处理的开源威胁情报基础信息。从近年国内外研究工作来看, 开源威胁情报的获取主要通过动态爬虫, 更新检测及话题检测等技术来实现。其中, 动态爬虫技术主要是将目标开源平台的信息动态完整抓取下来并存储。近些年来随着各大网站反爬虫机制不断加强, 开源威胁情报采集技术也在完善演进。文献[18]提出了一种基于卷积神经网络(Convolutional Neural Networks, CNN)的威胁情报自动识别模型。在该模型中, 利用爬虫技术从安全论坛和博客等平台获得非结构化语义文本数据, 并利用 CNN 框架实现了开源威胁情报的自动化判别提取。文献[19]提出了一种基于社交媒体数据的开源威胁情报自动提取和评估框架 TIMiner。在该框架中, 利用爬虫技术从博客、黑客论坛帖子等不同社交媒体平台收集威胁相关数据, 并利用自然语言处理(Natural Language Processing, NLP)和 CNN 实现带域标签 OSCTI 提取。除上述研究成果, 另外有大量研究如文献[20-23]等将动态更新及话题检测应用至动态爬虫技术中, 以提高威胁情报的爬取准确率。这些研究工作大都先利用爬虫技术获取目标数据, 并结合话题检测技术过滤掉与 IOC 无关的非结构化信息内容, 在实际部署中还利用了动态检测更新技术实时跟踪目标内容源, 以保证爬取内容的及时性。这其中话题检测技术是开源情报信息采集的关键技术, 近年来较为常用的技术方法主要采用命名实体识别(Named Entity Recognition, NER)结合支持向量机(Support Vector Machine, SVM)、逻辑回归(Logistic Regression, LR)、随机森林(Random Forest, RF)等机器学习分类方法。

上述研究工作将开源威胁情报采集通过动态爬虫与检测更新以及话题检测流程技术实现, 为落地实现开源威胁情报采集应用提供了很多有益借鉴。开源威胁情报采集只是威胁情报挖掘的基础, 需要进一步展开标准化或非标准化开源威胁情报的识别提取, 拓展获取开源威胁情报后的应用维度。

3.2 开源威胁情报识别提取

开源威胁情报识别提取是开源威胁情报挖掘的核心工作之一, 主要以非结构化开源威胁情报基础信息数据作为输入, 输出是标准化或者非标准化开源威胁情报, 涵盖了 IOC 提取与威胁情报生成等技术环节。由于不同的开源信息平台中披露的开源威胁情报内容结构存在较大差异, 其对应的威胁情报

识别提取方法也存在区别。接下来本节以不同开源威胁信息平台源为划分依据, 对开源威胁情报识别提取研究工作进行了归纳介绍。

3.2.1 技术博客

技术博客是面向广大较专业人员的技术问题、经验等分享交流学习平台。相较于社交媒体微博等, 其面向人群广度和内容传播时效较低, 但内容更为丰富且具有一定深度, 一般具有较强的专业性, 通常能够以更规范的形式为对象提供内容信息支撑。安全相关博客文章是开源威胁情报内容的重要载体之一, 其发布安全领域相关知识信息对预测现实世界漏洞利用、检测威胁、威胁预警等具有重要作用。针对安全相关的技术博客, 文献[24]提出了一种基于神经网络序列标记的端到端模型, 用于从网络安全技术文章中自动识别 IOC。在该模型中, 运用自然语言处理的序列标记技术从网络安全技术文章中收集本地代码, 同时结合多路聚焦(Self-attention)技术以更好地从网络安全技术文章文本中收集出上下文信息。实验表明, 该模型在自动识别 IOC 时具有良好的性能, 显著优于其他模型。文献[21]设计实现了一种基于大规模现场数据处理模型, 用于从安全相关技术文章中自动提取 IOC。该模型在自动提取 IOC 的同时还能将 IOC 关联至相应的活动阶段, 例如诱饵、开发、安装和指挥控制等阶段。通过实际大规模现场数据测试, 该系统在提取 IOC 和确定 IOC 活动阶段时均具有良好的性能。但不能以自动化方式记录 IOC 语义等信息, 因此安全人员需要手动提取和报告定性活动特征, 效率较低, 不具备普适性。文献[25]提出了一种自动从技术文章中提取 OpenIOC 格式开源威胁情报的技术 iACE。在该研究工作中, 作者利用图挖掘技术分析 IOC 标记及该标记与其所在句子上下文的关系, 当标记间的语法连接与通常表达 IOC 的方式一致时, 则提取 IOC 生成描述指示符(例如, 恶意 zip 文件)和其上下文(例如, 从外部来源下载)的 OpenIOC 标记。该技术利用 IOC 相关文章的语义特征并配合捕获实体间关系的图挖掘技术来提升 IOC 提取的准确性, 相较同期其他 IOC 工具, 其在性能上有一定优势, 对 IOC 提取技术的演进具有相当影响力。以上研究文献针对从技术博客中安全技术文章上定向识别提取开源威胁情报, 在可处理的信息源内容形式上比较单一。文献[18]提出了一种基于卷积神经网络的模型, 能够从安全方向技术博客中的所有非结构化数据中自动识别开源威胁情报, 突破单一的安全技术文章内容形式。该模型利用网络爬虫技术获得非结构化语义文本数据, 对获取到的语义文本进行预处理并输入到单词嵌入模型中用于提取特征向量, 最后应用 CNN 分类模型来识别 OSCTI 实体。经验证该模型在多个核心指标上优于其他模型, 能够提高 OSCTI 来源的覆盖率和识别准确率等指标。但由于训练集相对较小, 该方法也存在召回率不高, 存在容易混淆某些术语的问题。文献[26]提出了另外一种利用深度学习方法从安全技术博客中提取 STIX 标准开源网络威胁情报的方法。在该方法中, 作者综合利用了 NLP 等一系列技术, 有助减少人工干预, 使网络安全专业人员更好地配置优化安全工具性能以最终提供最佳防御。

3.2.2 社区论坛

社区论坛是面向所有网民群体的交流平台, 虽然专业性不及技术博客, 但内容、主题、形式更为丰富且传播速度也更为快捷。其中, 暗网深网等黑客社区论坛为黑客等提供一个自由言论的交流平台, 其中可能经常涉及大量有价值的威胁情报信息。鉴于此, 来自佛罗里达大西洋大学的团队[27]首先提出了一种针对暗网信息内容的预处理概率模型, 能够识别并过滤错误配置的流量以提高暗网数据纯度, 有效提升开源威胁情报的获取及存储效率。来自美国亚利桑那州立大学的团队[28]又提出了一种从暗网和深网上的站点收集开源网络威胁情报的原型系统, 该系统能有效收集高质量的网络威胁警告, 这些威胁警告包括关于新开发的恶意软件和尚未在网络攻击中部署的漏洞的信息, 可帮助安全专家进行更好的威胁分析应对。来自挪威科技大学的团队[29]为帮助信息安全响应团队将其审查重点放在最具情报价值帖子上, 提出了一种利用监督机器学习算法对黑客论坛帖子进行分类的方法, 以快速筛选出黑客论坛中不同类型的高质量开源威胁情报。为提高开源情报识别精度, 该团队[30]又进一步提出了一种基于狄利克雷分配(Latent Dirichlet Allocation, LDA)的混合机器学习模型对情报信息内容的聚类效果进行改进。通过使用实际黑客论坛数据进行测试, 结果表明该方法可快速准确地提取相关可操作情报。上述四项研究工作有助于安全人员更具有针对性地高效从暗网深网中识别提取高质量开源威胁情报。不同于此, Zhang 等人[22]认为 IOC 提取可认为是一个从旧威胁情报到新威胁情报的循环提纯过程, 并设计实现了一个从网络社区论坛中自动挖掘 IOC 信息的工具 iMCircle。该工具可从搜索结果中主动提取特定威胁域作为后续检索输入, 并在检索过程中自动判定提取目标是否和输入指标保持一致, 以实现开源 IOC 的动态收集。

总体来看, 通过暗网、深网等社区论坛形式进行开源威胁情报挖掘是一种可行技术。但由于暗网等社区论坛用户交互的匿名性, 使其发布的情报信息质量上也存在较大的不确定性, 需要大量的后期质量评价及验证工作。

3.2.3 社交媒体

Twitter 等社交媒体提供了一个庞大而多样的用户群, 是典型的开放信息内容自然聚合器之一, 且由于其依附于社交网络, 平台信息内容天然具有交互性高, 覆盖广泛, 时效性强等特性, 且能够汇集大量与网络安全相关的资源。基于社交媒体的这些特性, 近年有大量研究工作基于社交媒体平台进行威胁情报的识别提取研究。Ritter 等人[31]通过实验证实了社交媒体是安全相关事件信息的宝贵资源, 同时, 他们提出了一种基于 Twitter 流的焦点事件提取方法来帮助安全分析师及时获取威胁新事件, 识别提取开源威胁情报。Sceller 等人[16]提出了一个针对 Twitter 流的自我学习框架 SONAR, 可用于实时检测、定位和分类 Twitter 中的网络安全事件, 有助于安全分析师快速识别提取开源威胁情报。来自里斯本大学的团队[32]提出了一种从 Twitter 获取信息的端到端模型。该模型使用卷积神经网络实现开源威胁信息接收处理和安全实体识别提取, 以帮助减少安全分析师自动化过滤大量不相关信息, 提高开源威胁情报识别提取效率。来自马里兰大学的团队[14]提出了一个从 Twitter 等社交媒体信息流中识别分析 OSCTI 的框架 CyberTwitter, 以帮助安全分析师及时从实时更新的社交媒体信息中获得各种可能的开源威胁情报。在该框架中, 作者使用安全漏洞概念提取器(Security Vulnerability Concept Extractor, SVCE)来提取与安全漏洞相关的术语, 将提取的情报以资源描述框架[33](Resource Description Framework, RDF)三元组的形式存储在网络安全知识库中, 并使用语义 Web 规则语言(Semantic Web Rule Language, SWRL)规则来推理提取的情报。上述三项研究工作均能帮助安全人员在从社交媒体数据中识别提取开源威胁情报时避免冗杂的工作, 但在提取效率上存在缺陷。为了进一步提升开源威胁情报识别应用效率, Zhao 等人[19]提出了一种基于社交媒体数据的新型带域标签的 OSCTI 自动提取和评估的框架 TIMiner。该方法综合利用了词嵌入和句法依赖技术。该框架带域标签的分类 OSCTI 可以实现个性化共享, 使用户只关注他们自己领域中的威胁信息, 可减少无关信息对用户的干扰, 而使其专注于对与威胁最相关信息的分析, 有利于安全专家聚焦于特定领域不同威胁的演变趋势, 并抓住攻击防御的核心。总体来看, Twitter 等社交媒体已成为开源威胁情报的重要来源, 但社交媒体中数据庞杂, 质量良莠不齐, 情报数据提纯、威胁事件发现技术等有助于提升开源威胁情报识别提取的效率。

3.2.4 公共报告

公共报告是指发布于网络平台中可被公开获取的涵盖安全、漏洞或威胁等主题的报告。公共报告通常由专业人员发布, 虽然时效性较差, 但在形式与内容上都具有很强的专业性, 直接或间接覆盖大量威胁情报信息。文献[34]利用各种 NLP 技术分析并研究了漏洞报告, 并开发了一种自动从互联网上收集物联网漏洞报告的工具 IoTShield。作者利用该工具实际收集和分析了分布在博客、论坛和邮件列表中的 7500 多份安全报告。测试表明从公共漏洞报告中识别提取开源威胁情报具有一定指导价值。南京大学的 Mu 等人[35]认为现有安全漏洞报告普遍存在重要威胁信息覆盖率不高等不足, 提出利用开放平台中不同用户人群的报告来弥补公共漏洞报告中信息不足的缺陷。以上两个工作主要针对漏洞报告收集, 分析以及对信息弥合的方法进行研究, 有助于专业人员从公共漏洞报告中识别提取高质量开源威胁情报, 但上述研究未实现从公共漏洞报告中识别提取开源威胁情报的完整流程, 来自马里兰大学的团队[36]提出了一种从公共代码库(如 GitHub [37]、GitLab [38]、bitbucket [39])报告的漏洞列表信息中直接挖掘关于开源项目和库的开源威胁情报的方法, 并对客户机上已安装软件的库和项目依赖关系进行跟踪。该方法能够在安全知识图中表示并存储开源威胁情报和软件依赖关系, 用于帮助安全分析师和开发人员在发现有关产品中使用的链接库和项目的任何开源威胁情报后, 从知识图中查询和接收警报。北卡罗来纳大学的团队[40]提出了一种从非结构化的威胁报告中挖掘开源威胁情报的方法 TTPtrill。该方法利用 NLP 和信息检索(Information Retrieval, IR)等技术从非结构化的威胁报告中自动提取威胁动作并以 STIX 格式构建战术威胁情报(Tctics,Techniques& Procedures, TTP)。随后该团队[41]又提出了一种自动将非结构化威胁报告转换为结构化开源威胁情报的方法 ActionMiner。该方法结合了 NLP 与信息论中的熵和互信息(Mutual Information, MI)度量这两种技术。相比仅使用斯坦福(Stanford)依赖解析器, ActionMiner 方法在提取网络威胁行动时具有更高的精度和召回率。总体来看, 从公共报告中识别提取开源威胁情报已经成为开源威胁情报的主要来源之一。

但公共报告通常存在信息不足的问题, 现有大部分研究还需要不断拓展新的技术方法, 用于提升从公共开源报告中挖掘高质量开源威胁情报的效率, 以帮助安全人员进行更及时的威胁防御。

3.2.5 通用方法

另外还有一些研究工作如文献[42-45]通过综合应用 NLP、机器学习、数据挖掘等技术实现从非结构化信息中提取开源威胁情报。这些研究成果并没有针对区分某个特定开源威胁情报平台, 其技术方法具有一定的通用性 Ramnani 等人[42]提出了一种利用 NLP 技术和模式识别框架来自动提取开源威胁情报的方法。该方法综合运用了目标利用、话题跟踪及推荐等技术, 以 STIX 结构为基础建模, 实现了威胁情报的大规模提取。崇实大学的团队[43]提出了一种基于 NLP、虚拟化结构和分布式处理技术的 OSCTI 提取分析系统。该系统还可使用所产生的数据作为输入值来递归地提取更多的数据。通过保存和管理提取数据之间的关系, 用以帮助安全人员使用这些数据来分析网络攻击。文献[44]提出了一种基于事件的 OSCTI 发现和分析智能框架, 在该框架中, 作者综合利用 NLP、机器学习和数据挖掘等多种技术进行研究实现。后一年, 在文献[45]中, 作者提出了一种轻量级可扩展的在线框架 IoCMiner, 用以自动从公共信息共享平台中提取 IOC。在该框架中, 作者结合使用了图论、机器学习和文本挖掘等技术。总体来看, 上述研究中介绍的通用方法虽然具有较好的平台覆盖性, 但由于在开源情报信息识别处理时没有充分考虑各信息平台的特点, 其处理效率上还有待提高。

从上述分析可以看出, IOC 提取是开源情报信息采集识别环节中最核心的研究要点, 主要研究从开源情报数据中提取威胁情报实体, 并根据安全含义, 完整其上下文和战略信息, 填补不一致带来的歧义等。IOC 提取一般采用命名实体识别技术或其他人工智能处理技术, 如正则表达式匹配[40], SVM 等, 针对预处理后的非结构文本信息进行遍历定位出 IOC, 并应用机器挖掘技术获取目标实体关系, 最终根据实际需要进行标准化威胁情报格式输出。开源威胁情报采集及识别有助于提升情报信息的广度及厚度, 加快从漏洞发现到针对检测的防护周期, 可更好应用于威胁狩猎, 恶意检测等深度挖掘分析防护手段中。

3.3 总结与讨论

本节将开源威胁情报识别提取研究工作划分为技术博客, 社区论坛, 社交媒体, 公开报告, 通用方法五个平台, 并对这些平台的开源威胁情报识别提取工作进行详细对比分析, 如表 2 所示, 其中每一行代表一项研究工作, 第 1 列代表该项研究的主要提取平台; 第 3 列为该研究主要的技术应用场景; 第 4 列是为实现该研究所应用的技术方法; 第 5 列为性能评估; 第 6 列为通过总结优缺点对该项研究工作的评价。

表 2 开源威胁情报识别提取相关文献分类总结对比

Table 2 Classification, summary and comparison of related research on OSCTI identification and extraction

分类	文献	技术应用场景	提取方法									性能评估	评价	
			NLP			关系模型构造			机器学习		其他		优点	缺点
			NER											
			正则表达式	其他	其他	图	其他	SVM	神经网络	其他				
技术博客	[24]	识别技术文章中 OSCTI	■						序列标记、BiLSTM	多头自注意力机制		精确率＞81% 召回率＞80% F1＞81%	在 IOC 识别任务中表现更好; 优于其他序列标签模型	仅能处理英语和汉语; 未集成语言上下文特征
	[21]	提取 IOC 并将其分类到相应活动阶段	■	Stanford CoreNLP	word2vec 词嵌入	■	树		■			精确率≥78.2% 召回率≥80.7% 覆盖率 86.2%	可自动重构活动语义; 研究数据开源	精确率有待进一步提高; 不能自动化记录 IOC 语义等信息

续表

分类	文献	技术应用场景	提取方法									性能评估	评价	
			NLP			关系模型构造		机器学习			其他		优点	缺点
			NER											
			正则表达式	其他	其他	图	其他	SVM	神经网络	其他				
社区论坛	[25]	提取 IOC 并生成 OpenIOC 开源威胁情报	■	LSTM (BiLSTM)+CRF	Stanford 依赖解析器、DOM 树构建	■	图	■		LR	TextRank	精确率 95% 覆盖率 90%	IOC 生成性能优异; 可提供攻击实例间内在联系	处理语言单一, 仅支持英语
	[18]	识别技术博客中 OSCTI			Bert 词嵌入				TextCNN			准确率 90.38% 精确率 89.78% 召回率 92.59% F1 91.16%	在准确性、召回率和 F1 方面优于其他模型	训练集较小, 召回率不高; 存在某些容易混淆的术语
	[26]	提取生成技术博客中 STIX 格式 OSCTI	■	Stanford NLP						■		精确率 70%	代码稳定; 监督模型开源; 工作可复制且可扩展	召回率不如预期; 训练数据集过小
	[27]	提升暗网数据纯度与 OSCTI 提取效率					概率模型					FNR 0%	不依赖任何硬阈值, 提供单独的可能性模型, 独立于流量源性质	用以模型选择的概率估计差异未得到很好评估; 未大量测量数据
	[28]	收集暗网深网中 OSCTI						■		LR、RF		精确率≥78% 召回率≥68% 覆盖率≥80%	可收集新型恶意软件和潜在漏洞的信息	用于数据收集的开源平台有待扩展
	[29]	快速筛选黑客论坛中 OSCTI			词向量表、word2vec、GloVe			■	CNN	■		准确率＞96.9% 精确率＞97.6% 召回率＞5.2% F1≥96%	高准确率, 高性能, 低复杂度	未探索其他神经网络效果; 只能处理英语帖子
	[30]	提取黑客论坛中 OSCTI 并聚类黑客帖子至讨论主题					LDA 主题建模	■				准确率 98.82%	提取快速, 更高效灵活	未能发现零日攻击帖子信息; 数据来源不广泛; 数据量不充足
	[22]	连续提取网络社区论坛中 IOC	■		HTML 文件转化			■		■		准确率 91% F1 90.46%	可连续生成 IOC	离线状态下性能不佳; 挖掘指标类型单一
社交媒体	[31]	证实社交媒体是安全相关信息的宝贵资源			■					半监督学习			在现实世界数据的实验中优于大多数以前工作	在未标记数据集中性能一般
	[16]	自动检测、定位和分类网络安全事件		关键字列表查询	GloVe								可预先检测、分类、监控网络安全事件; 扩展定制性强	容易被有组织的用户群滥用, 捕获“假事件”

续表

分类	文献	技术应用场景	提取方法									性能评估	评价	
			NLP			关系模型构造		机器学习			其他		优点	缺点
			NER											
			正则表达式	其他	其他	图	其他	SVM	神经网络	其他				
社交媒体	[32]	处理开源威胁信息并识别提取安全实体		■	■				CNN、BiLSTM			TPR 94% TNR 91% F1 92%	专注性高; 性能优异	在基于非安全相关文本预先训练的嵌入向量时性能一般
	[14]	OSCTI 识别分析					网络安全本体 UCO[46]、语义网络 RDF 与 SWRL					准确率＞86%	实时性强	数据来源不广泛; 测试数据量不充足; 生成的网络安全警报的质量有待提高
公共报告	[19]	抽取 IOC 并提取评估新型带域 OSCTI	■	BiLSTM+CRF	word2vec、Stanford CoreNLP							准确率＞84% 召回率 92% F1 93%	产生带有域标签的 OSCTI; 有效识别未知 IOC	IOC 抽取方法基于非监督方法, 依赖于大量数据
	[34]	收集分析漏洞报告	■		Stanford CoreNLP						蜜罐	精确率≥97% 召回率≥83% FPR≤0.06% 运行时间 0.75s	时间成本低; 攻击成功的门槛较为容易	系统性能严重依赖于漏洞库; 蜜罐数据的质量不佳
	[35]	证明漏洞报告普遍缺少信息并提出弥合漏洞报告差距的建议					人工经验测量验证					整体成功率＞23% 漏洞重现率 95.9%	部分数据集可共享; 能有效实现内存错误漏洞信息弥合	需要进一步研究来检验统计结果如何推广到其他类型漏洞
	[36]	提取 OSCTI 并跟踪客户机上特定关系				■	网络安全本体 UCO						可进行安全知识图推理并生成警报	开源挖掘代码库支撑不足
通用方法	[40]	提取 STIX 标准 OSCTI			词性标记						TF-IDF 算法	精确率≥84% 召回率≥82% F1≥76%	可自动提取丰富的 TTP 信息	NLP 解析器性能和准确性有待提高
	[41]	提取结构化 OSCTI			词性标注		熵和互信息					精确率 92% 召回率 93%	精度和召回率优于斯坦福类型依赖解析器	各种威胁动作表达式不可自动解析
	[42]	提取 OSCTI		■	■						Basilisk 算法[47]	精确率＞50% 召回率＞80%	自动化处理程度高	处理不同非结构化文档之间的精度差异大
	[43]	提取 OSCTI			■						虚拟机、分布式处理技术		数据来源广泛; 数据处理能力强	数据分析非自动化

续表

分类	文献	技术应用场景	提取方法										性能评估	评价	
			NLP			关系模型构造			机器学习			其他		优点	缺点
			NER		其他	图	其他	SVM	神经网络	其他					
			正则表达式	其他											
	[44]	生成分析 OSCTI	■	Stanford NLP			图	■			TF-IDF、TextRank	精确率≥76.9% 召回率≥75%	在数据过滤和信息提取方面具有良好的性能	实验数据集不充分
	[45]	提取 IOC	■			■				RF		准确率＞97%	轻量级; 可有效提取未被披露的新 IOC	处理时间较长, 实时性不强

综合表 2 的对比分析可以看出, 已有开源威胁情报的获取及识别提取研究文献大多综合利用 NLP、关系模型构建、机器学习等数据挖掘技术从技术博客、社区论坛, 社交媒体, 公开报告等开源信息平台中实现威胁情报信息提取, 本质上是基于数据挖掘的信息萃取。相较于 BiLSTM+CRF 等方法, 很多研究文献在实体识别时更倾向于选择易实现的正则表达式。在关系模型构建时, 多运用图, 甚至引入专属安全领域的网络安全本体 UCO。而在机器学习分类时, 多选择算法简单, 鲁棒性强的 SVM。神经网络由于具有自学习、联想存储功能与高速寻找优化解等优势, 可以预见其未来在针对开源威胁情报挖掘中的应用占比会进一步扩大。本节以上内容有助于研究学者和相关从业人员快速了解开源威胁情报的识别提取, 同时促进在未来的研究工作中根据性能和优缺点等更准确高效的选择适当的方法从对应平台和技术应用场景中识别提取开源威胁情报, 完成目标安全求解问题。研究开源威胁情报识别提取技术, 有利于解决传统威胁情报开发的局限, 扩充商业威胁情报的数据维度, 为深入理解威胁攻击提供更为广阔有效的路径。但与此同时, 开源威胁情报采集来源广泛混杂, 情报质量不一, 需要强化开源威胁情报融合评价的研究, 以提高开源威胁情报的质量与可信性。

4 开源威胁情报融合评价

高质量威胁情报一般具备时效性、准确性、完整性、丰富性、可操作性、场景相关性等特征。现有开源威胁情报大多呈多源异构性, 情报质量良莠不齐, 这也阻碍了开源威胁情报的存储和共享, 应用于实际场景检测时也可能引发漏报、误报等不可控问题。开源威胁情报的融合评价为甄选高质量的开源威胁情报提供了数据融合方法与质量评价机制, 可满足威胁检测等现实需求。本节从开源威胁情报数据融合和质量评价两个方向展开文献收集, 并重点依据质量评价的定性评价方法和定量评价方法进行文献甄选和分析。其中当前威胁情报的数据融合研究工作多采用针对开源威胁情报的基础信息数据, 运用多源异构情报的一致性分析[48]和去伪去重等粗粒度数据融合方法, 通过拓展情报信息维度等操作, 实现对分析研判后的开源威胁情报归一化封装输出。开源威胁情报的质量评价研究是针对开源威胁情报的可信性及可用性等指标进行评估, 一般包括定性评价方法和定量评价方法。接下来我们对开源威胁情报数据融合和质量评价研究工作进行具体论述。

4.1 开源威胁情报数据融合

开源威胁情报由于情报来源的开放性, 也导致其情报产出具有显著多源异构性, 该固有弊端也阻碍了开源威胁情报的存储、共享和应用。开源威胁情报的融合处理是情报能够有效利用的前提, 近年来众多学者也对该方向做了大量研究, 目前已有研究主要通过对多来源本体相同的开源威胁情报进行一致性分析、去伪去重及数据融合分析等操作进行改善。

4.1.1 一致性分析

一致性分析的重要技术是本体构建, 本体是同一领域内不同主体之间进行交流以及连通的语义基础[49], 本体由多个元素构成, 其形式化定义[50]如下:

$$v=\left(C, R, H^{C}, rel, A^{v}\right) \tag{1}$$

其中, C 是本体概念的集合(通常使用自然语言进行

描述); R 是非上下文关系, 其中 $rel:R\to C\times C$ 定义了实际关系的映射; $H^C\subseteq C\times C$ 是上下文关系的集合, 定义本体的层次结构; A^y 是本体上公理的集合。其构建层次如图 4。安全情报本体作为情报知识图谱构建的核心层次, 是将信息抽取得到的实体及其关系构建为知识网络, 实现数据向知识的转化以及知识与应用结合的过程, 同时利用本体中定义的约束与规则可为后续的质量评估、知识推理等过程提供基础[51]。本体构建、一般基于本体复用, 本体构建和本体匹配等[51]的实现。从网络安全研究的原理、需求、规范等抽象角度进行构建的本体被称为基于模式的知识本体, 而从现有数据的格式、内容、结构化程度出发构建的本体则区分为基于数据的知识本体。北京航空航天大学的团队将本体应用于开源威胁情报一致性分析中, 提出了一种用于描述多源异构开源威胁情报的基于本体的统一模型[52], 以促进开源威胁情报的共享与分析。同时, 他们还进一步提出了一种基于统一模型和开源情报收集工具 IntelMQ 的开源威胁情报集成框架。

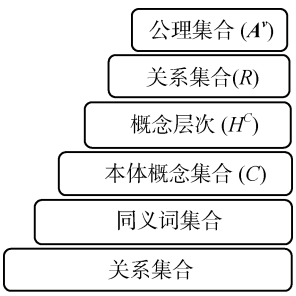

图 4 本体构建层次

Figure 4 Ontology construction level

4.1.2 去伪去重

开源威胁情报去伪去重是开源威胁情报挖掘时另外一个重要处理步骤, 主要使用维度扩展及挖掘分析等方法对情报数据进行提纯判定, 尽可能对基础情报信息进行增值。M. Adithya 等人[53]认为安全的信息去冗技术可以降低分布式存储中的通信和容量开销, 并在这个以信息为导向的大社会中有巨大应用。他们的观点证实了数据去重对开源威胁情报系统的重要性。Edwards 等人[54]就在一项美国专利中提出了开发一种可过滤、分类、消除重复数据、对数据项进行优先级排序的威胁情报系统的想法。Brown 等人[55]认为开源威胁情报系统在使用前必须对开源情报数据进行去重等操作, 避免将新收集的情报数据直接关联到现有数据, 以避免增加安全运营人员的额外工作量。其中去重操作主要是利用快速匹配算法从各种数据集中精准识别出匹配记录, 并将其从属性、关系或数据内容等维度上进行合并。作者同时也指出去重效果受到许多因素的影响, 包括数据质量、首字母缩略词和缩写词的不同用法或语言差异。

4.1.3 数据融合分析

开源威胁情报数据融合分析旨在通过运用机器学习等智能数据融合方法针对原始情报信息进行关联融合处理, 以获得具备时效性、准确性、完整性等特性的高质量威胁情报。目前学术界已产出一些威胁情报的数据融合分析成果。Modi 等人[56]于 2016 年提出了一个自动开源威胁情报融合框架, 该框架由分析、收集、控制、数据和应用层面构成, 它可从不同情报来源提取开源威胁情报并利用聚类技术对内容相似的情报数据进行聚合关联, 最终输出形成统一格式的威胁情报。Azevedo 等人[57]也提出了一种开源威胁情报关联融合的类似方法。该方法主要采用簇聚合技术, 可关联并聚合不同开源情报源中的相似 IOC 信息并将其汇集成簇从而得到提纯的开源威胁情报。文献[58]结合自然语言处理方法和智能分析技术, 设计实现了一种基于多源情报信息融合的高质量开源威胁情报生成工具。该工具综合运用一致性分析, 去伪去重等常见的粗粒度数据融合分析手段, 并结合了 SVM、贝叶斯推断等高阶数据分析技术, 可针对威胁情报数据进行清洗、集成、整合处理。但其数据融合方法手段及关联应用效率还尚待进一步提升。综合来看, 现有基于开源威胁的数据融合研究大都还处于采用一致性分析、去伪去重等粗粒度阶段, 也有部分研究借鉴并应用了一些高阶数据融合方法, 但其处理效率还待提升。传统的数据融合分析技术, 如贝叶斯推理、卡尔曼过滤等基于概率的方法, D-S(Dempster-Shafer)理论等证据推理方法, 机器学习、智能聚合、模糊逻辑等基于知识的方法等[59-60]具有质量好、稳定性强、鲁棒性高等优势, 非常适用于大数据环境中时效性要求高的开源威胁情报数据融合处理, 可应用于新兴的综合性数据融合分析以实现开源威胁情报融合。另外, 未来可预见开源威胁情报数据将趋于更庞杂, 基于深度学习的数据融合方法[61]由于其在处理海量数据上的优势, 也将得到广泛应用。

4.2 开源威胁情报质量及可信性评价

开源威胁情报用于辅助支持决策或安全分析, 情报的可信及可用性将直接影响安全决策分析结果。对情报质量的筛选、评估显得尤为重要, 国内外研究学者已展开了广泛研究工作, 一般可分为定性

评价方法和定量评价方法, 其中定量评价又包括特征指标提取, 指标自定义和应用图挖掘技术的方法。

4.2.1 定性评价方法

Bouwman 等人[62]将若干情报供应商提供的商业情报与开源数据进行了对比, 发现商业情报和公开情报在情报内容方面几乎没有重叠, 并指出商业威胁情报质量存在覆盖率不足, 及时性欠缺等问题, 这也从侧面说明了开源威胁情报可作为商业情报的有效补充。与此同时, Bouwman 还给出了一种商业威胁情报质量的定性评估方法, 主要利用了情报的场景相关性、丰富性、可操作性等特征。这些质量评价指标也可以作为开源威胁情报质量的有益借鉴。Alessandra 等人[63]提出了一种面向开源网络威胁情报平台的定性质量评估方法。该方法首先根据 5W3H(what, who, why, when, where, how, how much and how long)原则, 得出四个主要实体——威胁、时间、威胁参与者和防御, 并从威胁情报应用周期中抽取了一些通用的评价标准指标, 如收集阶段需要的通用格式, 分析阶段的数据模型和关系机制, 部署阶段所需要的情报数字签名格式等, 同时针对 OSCTI 平台, 还给出了一些额外标准, 如文件数量、质量以及许可证声明等。这些定性的评价标准或方法为提升开源威胁情报的可用性提供了有效途径。

4.2.2 定量评价方法

定性评价对于开源威胁情报的质量评价来说仍不精确, 因此有研究人员提出利用定量指标对开源威胁情报进行评价。

一些文献从开源威胁情报的特点出发, 提取多个特征作为评价依据。文献[64]基于 Lucassen 等人提出的信息可信度 3S(Semantic, Surface, and Source features)模型和情报共享的多源协作, 提出了开源威胁情报可信度多维度的分析方法。3S 模型指出信息特征和用户特征可共同作用来判断信息可信度, 其中信息特征有语义内容、表面特征和源特征等, 用户特征包括用户自身的领域知识和技能及相关经验。通过对此模型进一步深化扩展, 作者从时间、内容和领域知识三个维度提取了情报源的权威度、可验证情报源数等 16 个客观定量可信特征, 并提出基于 DBN(Deep Belief Network)的情报可信判别算法, 分析挖掘情报间不同维度下可信评价的关联关系。文献[64]还进一步总结得出, 开源威胁情报本身具有时效性。从时间维度看, 情报发布时间距离当前时间越近, 及时性越强, 其可信度就越高, 对预测当前企业、设备的威胁态势越有利; 从情报内容维度看, 开源威胁情报内容的文本格式和数据形式的机器可读性以及是否符合 STIX 或 OpenIOC 等标准, 可以反映情报的可用性和通用性。各个情报内容的相似度、贡献度可以反映情报的原创性、完整性; 从领域知识维度看, 开源威胁情报必须对威胁有定制化的全面分析, 包含大概率会出现的情境, 能够从海量情报中筛选出真正相关的情报, 尽可能地分析攻击的所有态势。在此基础上, 文献[65]分别从情报来源、情报内容、活跃周期、黑名单库匹配程度 4 个维度提取特征作为评估情报质量的依据, 设计了一套基于深度神经网络算法和 Softmax 分类器的情报质量评价模型。从情报来源维度看, 开源威胁情报的来源或载体的可信度在很大程度上可以直接反映该情报的可信程度。

另外有些学者提出了一些自定义的定量情报评价标准。Vector 等人[66]定义的度量标准包括数量、差异贡献、排他贡献、相对延迟、准确性(误报率)、覆盖范围。Thomas 等人[67]将开源情报的应用周期视为一个封闭系统, 对威胁情报的扩展性、保持性、误报率、可验证性、互用性、兼容性、相似性、时效性、完整性等 10 个定量参数进行了定义与推导, 采用加权平均模型, 使每个实体能够根据自己的需求和优先次序对参数进行调整, 并可通过应用结果对情报源质量的信任程度进行动态反馈调整。Schlette 等人[68]将威胁情报的评价维度划分为三个层次: 属性级、对象级、报告级。通过加权平均各个维度的聚合质量指标, 形成一个可量化的威胁情报质量评估体系。在该体系中, 每个定量维度的权重可调整, 且必要时可将人工 OSCTI 分析人员纳入质量评估体系。Griffioen 等人[69]提出了四种类型的威胁情报质量评价指标: 及时性、敏感性、原创性和影响力, 并基于这四种类型评价指标, 引入了一种改进分类方法对威胁情报实现定量评估。文献[70]则认为开源威胁情报本质是为用户提供检测服务, 提出了一种基于用户视角建立对应的定量指标体系, 对开源威胁情报服务进行评估的方法。该方法将威胁情报视为一种特殊服务, 其质量评价包括价格、功能、性能和质量、服务、资格等五个维度, 且基于人们更容易相信绝大多数人给出的信息真实性的假设, 提出基于多数威胁情报使用者的意见和评价来衡量情报的可信度。该方法可根据用户反馈来动态调整各检测项目的权重和得分, 以获得更为精确的情报质量评价结果。由于开源威胁情报在共享及应用时存在部分用户的“搭便车”行为。针对这一问题, Omar 等人[71]提出情报质量指数(Quality of Indicators, QoI)的概念, 用于评估开源威胁情报共享参与者的贡献水平。QoI

评估方法涉及的指标包括正确性、相关性、实用性和唯一性, 采用基准方法定义, 并利用机器学习算法进行质量评价。

利用图可直观有效地表达推断出各实体间的关系, 因此一些学者也提出应用图挖掘技术来进行情报评价方法研究。文献[72]首先提出从图挖掘的角度自动评估异构开源威胁情报的可信水平, 创新性地构建了异构开源威胁情报图, 并从源、内容、时间和反馈的多维角度提出了一种基于图挖掘的情报特征提取方法, 结合随机森林算法训练分类器, 为大规模异构开源威胁情报提供了一种自动可解释的可信评估方法。Roland 等人[73]提出了一种 OSCTI 源排序方法 FeedRank, 其核心思想即用相关图模拟 feed 之间的时间与空间关联, 根据内容的原创性和其他源对其引用的程度对源进行排名。此方法还会对每个 OSCTIF(OSCTI Feed)的贡献度进行量化分析。文献[74]提出了一种基于知识表示算法 TransE 模型和循环神经网络 RNN 模型的情报数据的可信评估模型。该方法利用了知识图谱在链接关系检索、关系存储等方面的优势, 构建了一个情报知识图谱, 并综合运用 TransE 和循环神经网络 RNN 模型对情报数据进行可信评价。

4.3 总结与讨论

本节总结论述了开源威胁情报的数据融合, 质量及可信性评价相关研究工作, 将质量及可信性评价相关研究工作划分为定性评价和定量评价两个方向, 并对依这两个方向收集甄选的开源威胁情报质量及可信性评价相关研究工作进行详细比较, 如表 3 所示, 其中每一行代表一项研究工作, 第 1 列代表不同的研究方向; 第 3 列为主要的技术应用场景; 第 4 列为实现该项研究所应用的技术方法, 主要从数学模型以及评价技术两个方向进行归纳分析; 第 5 列为性能评估; 第 6 列为通过总结优缺点对该项研究工作的评价。

综合表 3 中的分析比较, 可以看出, 机器学习神经网络等作为一种有效的分类工具, 已经被大量应用至开源威胁情报质量的定性评价中, 如文献[64-65]在多维度提取特征指标并都应用了机器学习中的神经网络模型; 而在定量评价中由于涉及各个指标的权重考量问题, 加权平均模型是更为常用的手段,

表 3 开源威胁情报质量及可信性评价相关研究分类总结对比

Table 3 Classification, summary and comparison of related research on OSCTI quality and credibility evaluation

方向	文献	技术应用场景	技术方法			性能评估	评价	
			数学模型		评价技术		优点	缺点
			数学定义与推导	加权平均模型				
定性评价	[62]	付费与公开资源比较			调查比较		大量实证分析数据	没有提出一种定量可应用的情报质量评估方法
	[63]	标准与平台评估			实体关系图、文献研究		从情报流程中推导出了通用评价标准	没有关注平台间互操作性的优势、互补平台的集成; 真实世界有效性还未验证
定量评价 特征指标提取	[64]	情报可信度多维度分析			DBN、词袋模型	准确率 92.31% 精确率 97.96% 召回率 85.71% F-score 91.43%	比传统算法的准确率和 F 值更高	评价指标的选取不够全面、具有代表性, 操作性不够灵活; 实验获取的训练样本缺乏全面性
	[65]	情报质量评估			Softmax、神经网络、NLP	精确率 91.37% 召回率 84.89% F-score 88.01%	与传统分类方法相比准确率和召回率均有很大提高	特征指标提取不够全面

续表

方向	文献	技术应用场景	技术方法			性能评估	评价	
			数学模型		评价技术		优点	缺点
			数学定义与推导	加权平均模型				
指标自定义	[66]	情报源评估	■			准确率>78.7% 覆盖率>85%	基础指标详实, 数据来源丰富	针对性不强; 缺乏参考标准
	[67]	情报源评估	■	■			可动态调整情报源评估参数, 自动化程度高	真实世界的有效性尚待验证
	[68]	情报质量评估	■	■			质量评估对共享平台的用户透明; 必要时可将安全分析人员纳入质量评估体系	度量指标不够全面; 缺少大规模环境的测试
	[69]	情报源质量评估	■			覆盖率>85%	实证分析; 情报来源丰富	评价指标不全面
	[70]	情报质量评估		■		准确率>80% 覆盖率>86.4	在覆盖率和区分度上具有明显优势	评价指标不够细化; 评价指标的权重值确定方法不够科学合理
	[71]	指标质量评估	■	■	机器学习、信息增益	准确率>72%	实际应用性强, 为具体程序和社区成员都分配了权重系数	指标权重值确定方法不够科学合理; 构建参考数据集需要花费大量人力
图挖掘	[72]	异构威胁情报可信评估			RF、SVM、KNN、CART、有向图、PageRank、子图同构、频繁模式挖掘、关联规则	精确率92.83% 召回率93.84%	对大规模异构威胁情报的可信评估自动 可解释; 可挖掘节点间的隐性关系	评价指标不够全面
	[73]	情报源排序			有向图、PageRank		强抗篡改性, 对大规模威胁情报处理具有较强的鲁棒性	度量标准不够全面
	[74]	威胁情报可信分析			RNN、BP、TransE、知识图谱、 资源分配策略	精确率91.67% 召回率85.71% F-score 88.59%	利用了知识图谱在链接关系检索、关系 存储等方面的优势, 可发现隐含或虚假的情报信息	没有针对匿名社交网络做情报信息可信分析

因此文献[68,70], 在针对情报的评估中, 都主要应用了加权平均数学模型对情报质量进行了量化评估; 有向图或知识图谱等技术可以充分挖掘情报之间的联系, 近年作为一种较为新颖的情报质量度量方法也受到广大学者关注, 例如文献[72-74]都利用了图挖掘方法, 其中文献[72-73]引入了有向图和 PageRank 算法, 而文献[74]则应用了知识图谱进行评估建模。以上对开源威胁情报的融合评价分析可以帮助相关研究人员和从业者展开源威胁情报质量融合与评价技术的研究, 并以此为基础提出一种综合的开源威胁情报质量定量评估方法, 可大大减少对开源威胁情报质量评价及可信度打分所需的人力, 为组织筛选出高质量、准确可信的威胁情报提供帮助。

5 开源威胁情报关联分析

开源威胁情报关联分析是指综合运用 Kill-Chain、钻石或异构信息网络等模型, 结合开源威胁情报信息, 对实时攻击流量数据进行深度关联、碰撞、分析等操作, 以期发现一些潜在的攻击行为, 进而推理挖掘揭示出隐含的攻击链条等高价值威胁信息。以开源威胁情报为应用核心的关联分析是当前开源威胁情报挖掘中的热点研究方向, 根据情报利用方式的不同, 可大致分为网络狩猎, 态势感知恶意检测三个应用场景, 本节依据这三个应用场景分别搜集并选取分析代表性的相关文献共计近 30 篇。其中威胁狩猎一般采用威胁情报驱动的检测方法, 针对网络流量数据进行主动搜索, 从而检测出可能

逃避现有安全防御措施的威胁目标。网络狩猎涉及图计算、模式匹配、领域特定语言等技术理论; 态势感知是以威胁情报大数据为基础, 从全局视角出发, 提升对安全威胁的发现识别, 理解分析、响应处置能力。由于涉及和恶意攻击行为的策略博弈, 因此在利用威胁情报进行态势感知分析时, 近期有较多文献引入了博弈理论来分析安全态势的发展。开源威胁情报的恶意检测则是指挖掘检测任何恶意侵害目标系统相关资产的代码或程序等。利用开源威胁情报辅助恶意检测有助于更快发现实体威胁目标。常见方法是从开源威胁情报中提取相关检测知识, 并与恶意软件的静态、动态特征数据进行关联, 构建网络安全知识图谱(Cybersecurity Knoweledge Graph, CKG)来挖掘恶意软件行为。接下来我们以网络狩猎, 态势感知和恶意检测这三个应用场景, 对开源威胁情报关联分析研究工作进行具体论述。

5.1 开源威胁情报网络狩猎

威胁狩猎[75]一般是采用人工分析和机器辅助的方法, 针对网络和数据进行主动和反复的搜索, 从而筛选出可能逃避现有安全防御措施的威胁攻击。与传统检测方式相比, 网络狩猎拓展了威胁检测方式, 可充分利用第三方威胁情报信息来提升对新型威胁的检测能力, 具有明确的目的性, 包括缩减威胁目标的狩猎范围, 显著减少威胁检测时间, 搜索发现未知威胁等。

如何获取准确、及时用多样化的威胁情报来提供大量辅助上下文检测信息是保证威胁狩猎成功的关键。现有网络狩猎技术需要大量的人工查询构建工作, 而忽略了 OSCTI 提供的关于威胁行为丰富外部知识。近年基于开源威胁情报的网络狩猎研究成果表明, 开源威胁情报可应用支撑威胁行为狩猎。文献[76]中提出了一种在计算机系统中使用 OSCTI 搜索网络威胁的系统 EFFHUNTER。在该系统中, 作者实现了一个无监督、轻量级和精确的 NLP 管道, 用于从非结构化 OSCTI 文本中提取结构化威胁行为, 同时作者为该系统匹配一个简洁而富于表现力的特定领域查询语言 TBQL, 用于搜索恶意系统活动, 提升猎捕效率。文献[15]提出了一种自动识别黑客论坛、IRC 频道和 Cardingshop 内潜在威胁的方法。该方法允许从收集的所有黑客内容中提取潜在威胁, 并通过将机器学习方法与信息检索技术相结合来识别系统中的潜在网络威胁。文献[77]设计实现了一种针对多个暗网数据源的 OSCTI 识别提取工具, 通过结合数据流量检测技术, 可实现威胁情报的快速集成、跨多个数据集的目标分析及威胁关联检测等操作。如何将威胁情报落地于旁路流量检测, 系统日志检测或主机行为检测产品中是威胁狩猎应用的难点问题。张等人[78]提出了一种新威胁情报平台 MANTIS 用以帮助安全分析师识别潜在威胁。该平台中运用基于属性图的相似性算法将不同的威胁数据形式统一表示。这种统一表示可方便安全分析师将不相关的攻击活动关联起来, 从而识别出可能的安全威胁。文献[79]将网络威胁搜索表述为图挖掘问题, 并提出了一个基于 OSCTI 检测的网络威胁狩猎系统 Poirot。该系统依托图挖掘关联技术, 将威胁情报和网络原始日志、终端日志、告警日志进行关联分析, 既可从攻击者视角完整揭示网络攻击活动的战术攻击路径, 也能从被控主机视角完整描绘被控主机网络行为, 呈现出威胁全貌。Kim 等人[80]提出了一种 OSCTI 收集管理框架 CyTIME, 可在无需人工干预的情况下自动生成入侵检测系统和恶意软件防御系统的安全规则, 用于实时识别新网络安全威胁。该工具能够高效自动为每个用户生成和存储安全规则。

除了上述对威胁进行识别搜索, 文献[81]提出了一种基于开源威胁情报数据进行实时识别威胁主题的方法。该方法能够在威胁检测平台边界中检测失陷主机, 同时增强流量的检测覆盖度。文献[82]提出了一个用于 OSCTI 建模和威胁类型识别的实用系统 HinCT。该系统设计一个威胁情报元模式来描述基础设施节点的语义关联, 进而在异质信息网络上构建网络威胁情报模型, 将各类节点关系的信息进行高级语义的集成。作者通过设计一种基于权重学习的元路径和元图的威胁基础设施相似度度量方法, 结合异质图卷积网络算法融合节点属性和基于元路径和元图的相似邻接关系, 从而识别基础设施节点的威胁标签。文献[83]认为对恶意资产的把握有助于威胁识别搜索, 进而提出了一种基于开源威胁情报的黑客社区恶意资产分析工具, 并运用深度学习算法及自学习检测模型对可能的内网渗透攻击进行主动搜索识别。文献[84]将主动威胁发现工作建模为图形计算问题, 通过运用威胁情报知识图谱技术实现了威胁事件的线索提取。该方法实现了一套自动证据挖掘和交互式数据检查的编程工具, 可用于以威胁情报数据为驱动的安全检测。

5.2 开源威胁情报态势感知

态势感知是以大数据分析为基础, 实现对安全威胁的发现识别、理解分析、响应处置, 从而完成对系统安全威胁的全局视角把控。一般来说, 为尽可能

从整体上动态掌握网络安全全局状况, 安全防御者需要尽可能引入外部信息来帮助其应对日趋复杂多变的新型网络威胁。开源威胁情报是一种基于环境的情报信息, 对于特定安全威胁具有靶向性。合理运用开源情报信息, 有利于快速感知发现网络威胁。基于这种认识, Husari 等人[85]提出了一种利用开源情报信息来感知探测 APT 攻击方法。该方法主要是利用博客、电子邮件和社交媒体等非结构化信息来提取并构建 TTP 链。具体来说, 作者利用 NLP 方法将非结构化的开源情报信息解构成标准 STIX2 格式的威胁情报, 结合机器学习方法解析推断出整个 APT 攻击的时间关系, 并通过流行的 ATT&CK 框架将情报内容翻译成可解释的 TTP 链, 可用于网络威胁态势的监测。上海大学的李等人[86]针对攻击链模型进行了仔细研究, 提出了一种基于 DNS 流量和开源威胁情报系统的 APT 探测模型。在该模型中, 作者以 DNS 流量作为 APT 整体检测的原始数据, 利用开源威胁情报信息测算整个系统 DNS 域名的风险值。国家互联网应急中心的温等人[87]提出了一种探测和预测 APT 攻击的方法。该方法综合运用情报收集、网络安全监控、基于知识的推理等手段对网络整体态势进行把握。实际测验表明该方法能够准确高效检测和预测 APT。总体来看, 现有利用开源威胁情报进行 APT 探测的研究工作中, 一个共性方法是利用博客、电子邮件和社交媒体等开源威胁情报信息来学习生成 APT 攻击链, 即各威胁动作的时序关系, 并基于此建立 TTP 模型来实现对 APT 攻击的快速感知和发现。

态势感知应用于系统安全防护时一般需要和具体业务流程结合, 而将开源威胁情报整合运用, 有利于改善业务流程的整体安全态势。Gschwandtner 等人[88]提出了一个在现有信息安全管理系统(Information Security Management, ISM)中集成 OSCTI 的框架, 以帮助组织增强其信息安全管理能力。该框架能使安全专业人员规划、集成和管理 OSCTI 内容, 同时辅助增强企业安全预算管理和企业网络弹性。一些新型网络攻击逐步瞄准关键基础设施中的工业控制系统。由于现有工控系统大都由各种 PLC 控制系统、网络系统及云系统混杂构成, 如何设计安全架构, 监控识别攻击, 实施动态威胁感知防御成为一个难点问题。南威尔士大学的团队[89]提出了一种基于 Beta 混合隐马尔可夫机制(Hybrid Hidden Markov Mechanism, MHMM)的新开源威胁情报态势感知架构用以监视识别来自工业 4.0 的网络威胁攻击。在该方案中, 作者对混杂物理和网络系统的工业 4.0 组件进行动态交互建模以实现监视识别功能。该机制在现实世界工业 4.0 系统中具有良好的适用性。

现有大部分利用开源威胁情报进行安全态势感知的研究工作, 都假设攻击及防御都为单次静态的, 并且威胁攻击总是出现在防御之前。而从现实情况来看, 随着攻防两端不断更新攻击及防御策略, 网络安全态势一直在处于此消彼长的动态变化中。博弈论结合开源威胁情报近年也被引入至威胁态势感知研究工作中。为帮助理解网络安全态势变化的趋势, 文献[90]提出了一种云计算环境下利用随机博弈和开源威胁情报的网络安全态势感知方法, 该方法利用博弈双方的效用来量化网络安全态势, 并探寻了该博弈模型的 Nash 均衡状态。文献[91]提出了一种基于开源威胁情报的网络攻击预测方法, 该方法基于攻击者和防御者之间的博弈关系, 结合高质量开源威胁情报中的上下文数据和攻防混合策略 Nash 均衡来预测攻击行为。文献[92]收集包含攻击媒介的大型国际黑客论坛, 使用深度学习文本分类来探测新兴的恶意移动软件变化趋势。该研究框架可以应用于探测其他黑客论坛资产, 以确定与用户相关的领域中的恶意软件趋势和主要传播者。文献[93]则充分利用来自经验测量的真实开源网络威胁情报, 并以轻耦合方式整合至业务系统。通过运用威胁情报, 业务系统可将网络和物理环境联合起来, 结合博弈策略来预测、推断和归因有形的计算机程序产品攻击, 以提升业务产品的安全性。文献[94]提出了一种基于开源威胁情报的社交物联网(Social Internet of Things, SIoT)账户恶意行为预测方法。该方法利用支持向量机获取与目标账户恶意行为相关的开源威胁情报, 分析开源威胁情报中的上下文数据关系来预测恶意账户的行为, 并探究了最终可能的平衡状态。在这些研究工作中, 开源威胁情报作为防御方的动作策略集, 是其预测潜在攻击行为的重要基础。而另一方面, 由于社交媒体、博客和黑暗网络漏洞市场等情报的多种语言特点, 阻碍了威胁情报的解析及预测效率。为更好利用开源信息进行网络态势感知, Ranade 等人[95]提出了一种基于神经网络的开源情报跨语言翻译系统。该系统使用多语言威胁情报系统来协调不同语言的网络术语表示, 帮助安全分析师及时理解并抓住多语言威胁情报中的关键信息, 从而扩展至全球范围内安全监控, 威胁预测感知能力。

5.3 开源威胁情报恶意检测

随着网络攻击中可利用的恶意工具或软件越来

越趋于常态化, 传统的基于异常和基于签名等的检测技术已经难以保证其检测时效性。开源威胁情报恶意检测旨在利用开源情报信息挖掘检测可能对目标资产造成损害的攻击对象, 包括恶意软件、恶意 URL 等。近年来国内外研究学者针对该方向也展开了大量的研究工作。Gandotra 等人[96]设计实现了一个可帮助安全人员分析、识别和预测恶意软件并进行早期预警的框架(Early Warning System, EWS)。通过该框架生成的威胁情报可以与安全机构共享, 以便安全人员发布建议和预防措施来应对未来的恶意软件威胁。在恶意软件识别中, 针对恶意软件进行甄别分类有利于更好了解恶意软件感染方式及威胁级别。胡等人[97]提出了一种基于开源威胁情报的恶意软件机器学习分类器。该方法通过开源情报信息来提取恶意软件中的多方面内容特征, 如指令序列及字符串等, 能够高效完成恶意软件检测分类。Piplai 等人[98]提出了一种开源威胁情报结合网络安全知识图谱进行恶意软件检测的方法。该方法的主要思路是将开源威胁情报中提取的知识与沙箱中捕获的恶意软件行为数据构建知识图谱, 并运用图挖掘技术来推断识别恶意软件行为。在恶意软件的识别检测中, 恶意对象的特征提取是其关键步骤。一个准确且具有良好表征意义的特征可有效提升检测效率。应用开源威胁情报对于准确提取恶意软件特征有良好的借鉴作用。来自美国马里兰大学的团队[99]提出了一种端到端特征集自动生成方法 FeatureSmith, 用以从安全会议发表的论文内容中自动提取用于训练机器学习分类检测器的特征集。该团队还利用 FeatureSmith 自动生成了一个用于检测恶意软件的特征集, 可集成到已有安全系统中为恶意软件检测提供便利。

恶意 URL 也是一种典型的恶意攻击载体, 当前主流的防御方法主要依靠黑名单机制, 其准确性及灵活性较差。引入机器学习方法来优化恶意 URL 检测是常见的解决方法, 但也存在由于 URL 的短文本特性所导致的特征单一等不足。中国科学院大学的汪鑫等人[100]提出了一种将开源威胁情报与 URL 检测相结合的思路, 并实现了一个基于开源威胁情报平台的恶意 URL 检测系统。该系统从开源情报信息源中提取出 URL 字符串的结构特征、情报特征和敏感词特征等三类特征, 辅以训练分类器, 并引入多分类器投票机制来提升分类精度。跨站脚本 XSS 攻击作为恶意 URL 的一种典型威胁, 传统检测方式一般依靠静态分析和动态分析。文献[101]提出了一种基于贝叶斯网络域内知识和开源威胁情报集成学习的 XSS 攻击检测方法。在该文中, 作者收集了大量开源威胁情报信息, 并用其生成模拟真实环境的 XSS 攻击检测数据集。实际实验表明, 该数据集可有效模拟真实场景。

恶意攻击会对数据安全、资产系统造成严重危害, 而攻击现场往往蕴含着有关攻击方的丰富信息。可采取数字取证分析得到恶意攻击来源、模式以及攻击方的画像, 以帮助改进系统后续防御效能。鉴于现阶段系统数据流量巨大, 攻击技术日趋复杂, 这些特性都给安全事故现场的数字取证带来困难。数字取证结合威胁情报信息有利于安全事件的调查取证和快速溯源。基于这种认识, Serketzis 等人[102]利用可操作的 OSCTI 基于已有的数字取证准备(Digital Forensic Readiness, DFR)模型开发扩展的轻量级 DFR 模型, 旨在实现快速有效的数据分类, 使响应者或取证分析师能够快速过滤掉与系统危害无关的数据类, 显著提高通过针对恶意活动模式的数字取证效率。为增强现有 DFR 方案的有效性, Serketzis 等人[103]又结合数字取证技术, 定量运用开源威胁情报数据来识别高取证价值信息, 以此用于快速分类和识别恶意软件的攻击模式。

5.4 总结与对比

本节具体介绍了开源情报关联分析的网络狩猎、态势感知和恶意检测三个重要应用方向, 阐述了依这三个关联分析应用方向搜集选取的代表性研究工作, 并对这三个关键应用方向中研究工作进行详细比较分析, 如下表 4 所示, 表中每一行代表一项研究工作, 第 1 列代表相关开源威胁情报联合分析研究被分类的三个主要方向; 第 3 列为每个研究工作的具体技术应用场景; 第 4 列为该项研究为实现任务所应用的具体技术方法, 主要从数据处理, 关系模型构建, 检测方法以及数据存储方向进行归纳分析; 第 5 列为性能评估; 第 6 列为通过总结优缺点对该项研究工作的评价。

综合表 4 的对比分析可以看出, 开源威胁情报关联应用的研究文献综合利用了机器学习、NLP、数据库等技术方法, 涵盖网络狩猎、态势感知、恶意检测等极为普遍的安全领域交互应用场景。从应用角度来看, 网络狩猎侧重于针对未知、新式、变异等攻击威胁的搜寻检测; 态势感知更关注于提升对全局威胁形势把握的技术手段的研究, 包括整体决策, 威胁分类, 攻击预测等。恶意检测则是针对可能对目标资产造成实质侵害的恶意对象实体, 如恶意软件、URL 和活动等。从技术实现角度来看, 相较网络狩猎以及恶意检测关联分析, 开源威胁情报态势感知

表 4 开源威胁情报联合分析相关研究分类总结对比

Table 4 Classification, summary and comparison of related research on OSCTI joint analysis

分类	文献	技术应用场景	技术方法				性能评估	评价	
			数据处理	关系模型构建	检测方法	数据存储		优点	缺点
网络狩猎	[76]	搜索网络威胁	NLP	威胁行为图构建[104-106]	依存句法分析	关系模式	精确率 100% 召回率 96.74% F1 98.34%	TBQL 专为威胁搜索设计,简洁高效; 高精度威胁提取	可能合成不合理的事件模式
	[15]	识别黑客论坛内潜在威胁			相关性排序、信息检索关键词搜索			采用不同方法针对性收集不同黑客论坛黑客内容	数据收集范围不广泛
	[77]	识别跨暗网数据源中威胁		多节点网络、Gephi 创建交互式网络仪表板		数据库		快速集成附加数据; 跨多个数据集实现目标分析; 自动化数字定位	自动爬虫和解析器相结合识别效果有待进一步证明
	[78]	识别威胁	simhash 算法	有向图、信息检索词袋模型			平均精确率 80%	全局威胁建模; 可协助安全分析师有效调查高危事件	不能检索未导入对象; 可能遭受规避攻击
	[79]	检测已知网络威胁攻击		源图构建 Gp 、查询图构建 Gq	图形模式匹配、图挖掘、图对齐		运行时开销≤ 1.86%	威胁搜索可靠快速高效, 更易检测变异攻击	互联网连接的受控环境中威胁搜索时间会增加
	[80]	生成威胁检测安全规则	XML 文件解析、STIX 2.0 格式转换			数据库	规则生成平均时间＜0.0481s	能够快速高效自动为每个用户生成和存储安全规则	安全规则映射算法不够通用
	[81]	识别威胁主题	域内 NER		TF-IDF 算法		准确率＞98% F-Score＞98%	可对特定领域主题或高复杂性主题产生较充分的特征表示	缺少支撑安全域实体数据库
	[82]	识别威胁类型		异质信息网络	GCN		Micro-F1 提高＞3%	显著提高威胁类型识别性能	异质信息网节点和边类型有待丰富
	[83]	恶意资产门户分析		隐含狄利克雷分布 LDA	SVM、余弦相似度			避免了被动的威胁信息收集分析	多种功能可被进一步开发
	[84]	将威胁发现建模来搜索威胁		图构建	图挖掘、τ 演算	分布式图形数据库	搜索平均时间≤0.47s	威胁检测分析能力强大高效	未实现完全自主
	[85]	APT 链学习	正则表达式、SMITRE ATT&CK 和 STIX 2.0 格式建构					可自动理解和响应非结构化文本中共享的网络攻击	使用英语时间锚无法捕捉到不可忽略的大量时间关系
态势感知	[86]	探测 APT		C4.5 决策树	K-Means	json 格式封装	检出率＞50%	对合法域名误判率较低	有部分符合正常语言习惯的恶意域名无法检出; 对 OSCTI 库信息的准确度要求高
	[87]	探测 APT 攻击			模糊推理、基于规则的推理	数据库	可靠性＞90%	有效准确预测 APT	需要依赖大量异常行为和数据
	[88]	ISM 流程增强	正则表达式		焦点小组讨论			可有效增强安全预算管理和企业网络弹性	需进一步实现将技术创新纳入 ISMS 各种其他流程的方法
	[89]	感知工业 4.0 网络威胁		Beta MHMM			准确率＞96% 召回率＞95% FPR＜4%	解决了基于规则的检测系统中固有的问题	依赖于大量正常、攻击样本; 滑动窗口性能效果有待验证

续表

分类	文献	技术应用场景	技术方法				性能评估	评价	
			数据处理	关系模型构建	检测方法	数据存储		优点	缺点
恶意检测	[90]	感知网络安全态势		随机博弈	虚拟机自省 VMI 机制			准确反映网络安全态势变化,预测攻击行为	真实环境中的可用性还未验证
	[91]	预测网络攻击		非合作博弈			情报匹配剩余比率＜18%	可筛选出相关外部威胁情报;充分考虑系统漏洞信息, 有效预测攻击	威胁情报匹配精度与速度有待进一步提高
	[92]	探测移动恶意移动软件趋势		二分网络	RNN(LSTM)、Adam 优化器		精确率≥95% 召回率≥81% F-Score≥87%	可发现未知的威胁行为者及其相关的威胁转移点	社交网络分析目标有待进一步扩展
	[93]	预测计算机程序产品攻击	蜜罐采集	图核[107]	阈值机制			结合了物理领域的威胁数据流与网络领域的攻击特征; 可提供明确的归因证据用于攻击预测	真实操作环境中的整合、可用性还未验证
	[94]	预测 SIoT 账户恶意行为			SVM		79.11%≤准确率≤80.13%	具有良好的泛化能力; 避免局部极小点和维数灾难	分类精度、实用性仍有提高空间
	[95]	跨多种语言翻译理解 OSCTI	Word2Vec 词嵌入	对齐模型[108]	RNN(LSTM)	数据库	准确率 97.22% 困惑度 4.07 BLEU 28.4	比第三方引擎更好记录了流行的网络安全术语; 可用于处理敏感情报数据时的私人操作环境	模型训练需丰富的网络安全语言知识; 知识获取代价昂贵
	[96]	识别检测恶意软件		统计建模	监督机器学习算法	数据库		具有在线和离线两种模式	未实现完全自主
	[97]	分类、识别恶意软件		N-gram 模型	哈希内核[109]、KNN、LR、SVM、RF		准确率 99.8% 对数损失 0.0258	准确有效将未知恶意软件样本分类到特定的家族	可扩展性需进一步提高
	[98]	检测恶意软件	NER	网络安全本体 UCO、CKG	SPARQL [110]查询语言、相关系数、机器学习			聚集了来自 OSINT 和恶意软件行为的数据, 可发现来自单个来源信息更多的信息量	用以获得 OSCTI 的 feed 不够充分; 未将生成的 CKG 导出到基于属性图的系统
	[99]	端到端恶意特征集自动生成	Stanford 依赖解析器	语义网络	过滤和加权技术		TPR 92.5% FPR 1%	可自动补充丰富的信息特征	不能自动识别与一些操作相关联的特征, 如“max”、“number of”
	[100]	检测恶意 URL		多分类器投票模型	决策树、贝叶斯、SVM		准确率 96% 召回率 87.1% F-Score 91.3%	提出针对 URL 的结构特征, 提高检测效果	多分类器模型训练参数未调整优化, 检测效果有待提高
	[101]	检测 XSS 攻击		贝叶斯网络	集成学习(bagging)		准确率 98.54%	可根据输出节点的影响对贝叶斯网络中恶意节点排序	数据集和实际测试场景需充实
	[102]	检测恶意活动模式		DFR 模型		图形和审计日志数据库	准确率 90.73% 精确率 96.17% 召回率 93.61%	可显著减少数字取证调查人员需检查的数据量	DFR 依赖的数据质量需提高
	[103]	分类和识别恶意活动模式		DFR 模型	弹性搜索	图形数据库、NoSQL		可减少对潜在威胁采取行动所需的时间	获取相关对象、运行评分算法等过程所需时间长

分析更多的应用了深度学习技术来进行全局威胁情势把握与预测。本章节梳理工作可帮助研究学者和从业者了解主流开源威胁情报的关联应用场景与方法, 快速确定研究方向或为已有安全问题提供解决思路。随着针对关键基础设施的威胁攻击日趋复杂, 开源威胁情报在威胁关联分析中将占据更加重要的比重, 亟需在已有基础上投入更多的人力物力精细化深入拓展开源威胁情报关联应用。

6 总结与展望

开源威胁情报具有种类多样、内容丰富、快速灵活等特点, 可作为直接或潜在安全威胁的外部鉴定信息资源, 有效提高网络攻击的检测识别与响应处理能力。本文聚焦于开源威胁情报挖掘应用技术, 系统梳理分析了近年来开源威胁情报挖掘相关工作的研究现状, 归纳总结出了开源威胁情报挖掘的一般流程框架模型, 并针对开源威胁情报识别提取, 开源威胁情报融合评价以及开源威胁情报关联应用三个关键场景进行了系统评述和优劣势分析。通过归纳总结分析现有研究成果, 本文发现开源威胁情报挖掘无论从信息源的拓展, 数据质量评价还是在安全防御中的应用价值, 都呈现快速发展的趋势, 但也存在一些局限性。现有这些局限问题的存在为未来开源威胁情报的发展提供了机遇和挑战。结合近几年的研究热点, 目前开源威胁情报挖掘研究工作的局限性及其发展趋势主要表现在以下几个方面:

(1) 面向学术研究的统一信息模型和框架

现有开源威胁情报挖掘研究主要局限于某个特定开源社区或者某个特定的社交平台, 其研究方法主要是按研究对象的不同进行具体区分, 学术角度看尚未形成具有明晰脉络的技术体系, 缺少从全局和共性的角度去考虑开源情报数据的信息模型及其挖掘问题的基础性研究工作。这种情况不利于该领域相似研究工作的继承、借鉴和比较, 也不利于该领域的长期发展和积累。从已有开源情报挖掘相关工作分析中不难看出, 很多开源情报挖掘问题都可通过应用命名实体识别技术或其他人工智能技术, 如正则表达式匹配, BiLSTM+CRF 等来进行实现, 不同的开源情报平台, 如社交网络、技术博客或研究报告等都完全可以共享同一个信息模型和基础算法。如何构建形成面向学术研究的统一信息模型和框架是一个重要问题。

(2) 面向数据投毒的情报应用风险评估

由于开源信息平台其固有的开放多源性, 使其威胁情报质量很容易受到错误信息干扰。例如攻击者可采用人工智能和机器学习等技术, 针对数据训练过程中的漏洞, 往目标训练数据集中注入“中毒数据”, 从而生成虚假威胁情报, 甚至迫使模型学习错误的输入以服务于攻击者的恶意目标, 来破坏网络防御系统。目前国内外对针对威胁情报挖掘领域中数据风险把控方面的研究相对较少。一方面是由于国内开源情报挖掘大环境还处于萌芽状态, 尚无有效的情报分析机制。由于不同挖掘模式下的数据类型和服务类型不同, 需要研究建立具有较好适应性、有效性的风险分析与评估模型, 而目前开源威胁情报挖掘领域在风险评估方面缺少体系研究, 知识积累不足。针对上述问题, 可研究和借鉴现有大数据、人工智能等领域的相关成熟技术, 结合威胁情报的自身特点进行深入的探索。

(3) 面向大众的开源情报开发支撑工具

开源情报挖掘主要采用大众生产模式, 越来越多的外部开发者通过公开发布方式在开源平台中贡献威胁情报信息。外部贡献已经成为开源威胁情报的主要推动力, 近年来在威胁情报中的比重呈不断增长趋势。限制开源情报发展的一个重要因素在于威胁情报生产具有相当的技术门槛, 这主要包括两个方面原因: 一方面, 包含威胁情报的安全流量数据一般存在于专用安全检测设备中, 如蜜罐、防火墙中, 难以轻易独立获取;另一方面, 即使获取到安全检测等数据, 也需要开发者具有威胁情报的专业知识来从中提取出威胁情报信息。研究一个面向大众的开源情报开发支撑工具, 实现对大规模异构流量数据条件下的快速威胁情报定位、提取, 并建立统一的威胁数据信息模型, 对于建立更为友好的威胁情报生态具有重要意义。

(4) 面向全环节的开源情报时效性提升

现有开源情报挖掘技术多通过爬虫等技术在开放信息源中进行遍历提取, 在性能指标中更关注于情报的准确性、覆盖性。随着网络威胁的更新迭代日趋频繁, 对于威胁情报的时效性指标也要求越来越高。现有开源威胁情报挖掘研究工作大都瞄准从某个具体环节对挖掘效率进行提升[111-120]。而实际上, 开源威胁情报深度挖掘的各个环节都在影响整体的速度效率, 提升威胁情报的时效性需要从整体上进行综合把握。例如开源情报信息源有很多是通过论坛, 社交网络等平台, 以流数据形式动态产生, 因此针对大规模动态开源情报网络信息, 通过研究高效的模型和算法, 来尽可能提升开源情报挖掘效率是一个重要环节。另外高质量的威胁情报本质来源于情报发布者的及时分享及发布, 这一般由情报发布

者自我驱动。如何设计合适的激励机制, 综合考量威胁情报的价值, 从而激励各个组织主动及时产出并共享更多的威胁情报是影响威胁情报质量提升的关键问题。而目前激励机制设计的首要难点是解决威胁信息数据价值评估难度大、威胁信息交易收益不易计量的问题。

网络技术日益翻新的今天, 开源威胁情报挖掘技术可缓解传统威胁情报信息量单薄等问题, 其研究发展得到了学术界和工业界的广泛关注。但是对开源威胁情报挖掘研究工作进行系统化梳理的相关研究成果并不多。本文对当前开源情报挖掘领域进行梳理, 重点分析了开源威胁情报从采集识别提取至融合评价再至关联分析交互场景应用的完整基于开源信息平台开源威胁情报挖掘流程, 并基于现有研究工作, 提出了当前开源威胁情报挖掘工作中存在的问题以及未来发展方向, 旨在为威胁情报应用及其他相关安全领域的研究和实践提供有益借鉴。

参考文献

[1] Threat Intelligence Reports. https://www.fireeye.com/current-threats/threat-intelligence-reports.html. 2014.

[2] Xu L P, Hao W J. Analysis and Enlightenment of US Government and Enterprise Cyber Threat Intelligence[J]. *Netinfo Security*, 2016(9): 278-284.
(徐丽萍, 郝文江. 美国政企网络威胁情报现状及对我国的启示[J]. *信息网络安全*, 2016(9): 278-284.)

[3] Hutchins E M, Cloppert M J, Amin R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[J]. *Leading Issues in Information Warfare & Security Research*, 2011, 1(1): 80.

[4] Landauer M, Skopik F, Wurzenberger M, et al. A Framework for Cyber Threat Intelligence Extraction from Raw Log Data[C]. *2019 IEEE International Conference on Big Data*, 2019: 3200-3209.

[5] Kurogome Y, Otsuki Y, Kawakoya Y, et al. EIGER: Automated IOC Generation for Accurate and Interpretable Endpoint Malware Detection[C]. *The 35th Annual Computer Security Applications Conference*, 2019: 687-701.

[6] Catakoglu O, Balduzzi M, Balzarotti D. Automatic Extraction of Indicators of Compromise for Web Applications[C]. *The 25th International Conference on World Wide Web*, 2016: 333-343.

[7] Urias V E, Stout W M S, Lin H W. Gathering Threat Intelligence through Computer Network Deception[C]. *2016 IEEE Symposium on Technologies for Homeland Security*, 2016: 1-6.

[8] Kumar S, Janet B, Eswari R. Multi Platform Honeypot for Generation of Cyber Threat Intelligence[C]. *2019 IEEE 9th International Conference on Advanced Computing*, 2019: 25-29.

[9] Sanjeev K, Janet B, Eswari R. Automated Cyber Threat Intelligence Generation from Honeypot Data[M]. Inventive Communication and Computational Technologies, 2020: 591-598.

[10] Afzaliseresht N, Miao Y, Michalska S, et al. From Logs to Stories: Human-Centred Data Mining for Cyber Threat Intelligence[J]. *IEEE Access*, 2020, 8: 19089-19099.

[11] Sabottke C, Suciu O, Dumitraş T. Vulnerability Disclosure In the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits[C]. *The 24th USENIX Conference on Security Symposium*, 2015: 1041-1056.

[12] Bozorgi M, Saul L K, Savage S, et al. Beyond Heuristics: Learning to Classify Vulnerabilities and Predict Exploits[C]. *The 16th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2010: 105-114.

[13] Khandpur R P, Ji T R, Jan S, et al. Crowdsourcing Cybersecurity: Cyber Attack Detection Using Social Media[C]. *The 2017 ACM on Conference on Information and Knowledge Management*, 2017: 1049-1057.

[14] Mittal S, Das P K, Mulwad V, et al. CyberTwitter: Using Twitter to Generate Alerts for Cybersecurity Threats and Vulnerabilities[C]. *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 2016: 860-867.

[15] Benjamin V, Li W F, Holt T, et al. Exploring Threats and Vulnerabilities In Hacker Web: Forums, IRC and Carding Shops[C]. *2015 IEEE International Conference on Intelligence and Security Informatics*, 2015: 85-90.

[16] Le Sceller Q, Karbab E B, Debbabi M, et al. SONAR: Automatic Detection of Cyber Security Events over the Twitter Stream[C]. *The 12th International Conference on Availability, Reliability and Security*, 2017: 1-11.

[17] Li M M, Zheng R F, Liu L, et al. Extraction of Threat Actions from Threat-Related Articles Using Multi-Label Machine Learning Classification Method[C]. *2019 2nd International Conference on Safety Produce Informatization*, 2019: 428-431.

[18] Xun S, Li X Y, Gao Y L. AITI: An Automatic Identification Model of Threat Intelligence Based on Convolutional Neural Network[C]. *The 2020 the 4th International Conference on Innovation in Artificial Intelligence*, 2020: 20-24.

[19] Zhao J, Yan Q B, Li J X, et al. TIMiner: Automatically Extracting and Analyzing Categorized Cyber Threat Intelligence from Social Data[J]. *Computers & Security*, 2020, 95: 101867.

[20] Xu L J, Zhai J T, Yang K, et al. A Multi-source Network Security Threat Information Collection and Packaging Technology[J]. Journal of *Network Security Technology & Application*, 2018(10): 23-26.
(徐留杰, 翟江涛, 杨康, 等. 一种多源网络安全威胁情报采集与封装技术[J]. *网络安全技术与应用*, 2018(10): 23-26.)

[21] Zhu Z Y, Dumitras T. ChainSmith: Automatically Learning the Semantics of Malicious Campaigns by Mining Threat Intelligence Reports[C]. *2018 IEEE European Symposium on Security and Privacy*, 2018: 458-472.

[22] Zhang P P, Ya J, Liu T W, et al. IMCircle: Automatic Mining of Indicators of Compromise from the Web[C]. *2019 IEEE Symposium on Computers and Communications*, 2019: 1-6.

[23] Huang L Z, Liu J Y, Zheng R F, et al. A Framework for Proactive Acquisition of Threat Intelligence Based on Darknet[J]. *Journal of Information Security Research*, 2020, 6(2): 131-138.
(黄莉峥, 刘嘉勇, 郑荣锋, 等. 一种基于暗网的威胁情报主动

获取框架[J]. *信息安全研究*, 2020, 6(2): 131-138.)

[24] Long Z, Tan L Z, Zhou S P, et al. Collecting Indicators of Compromise from Unstructured Text of Cybersecurity Articles Using Neural-Based Sequence Labelling[C]. *2019 International Joint Conference on Neural Networks*, 2019: 1-8.

[25] Liao X J, Yuan K, Wang X F, et al. Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence[C]. *The 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016: 755-766.

[26] Ghazi Y, Anwar Z, Mumtaz R, et al. A Supervised Machine Learning Based Approach for Automatically Extracting High-Level Threat Intelligence from Unstructured Sources[C]. *2018 International Conference on Frontiers of Information Technology*, 2018: 129-134.

[27] Bou-Harb E. A Probabilistic Model to Preprocess Darknet Data for Cyber Threat Intelligence Generation[C]. *2016 IEEE International Conference on Communications*, 2016: 1-6.

[28] Nunes E, Diab A, Gunn A, et al. Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence[C]. *2016 IEEE Conference on Intelligence and Security Informatics*, 2016: 7-12.

[29] Deliu I, Leichter C, Franke K. Extracting Cyber Threat Intelligence from Hacker Forums: Support Vector Machines Versus Convolutional Neural Networks[C]. *2017 IEEE International Conference on Big Data*, 2017: 3648-3656.

[30] Deliu I, Leichter C, Franke K. Collecting Cyber Threat Intelligence from Hacker Forums via a Two-Stage, Hybrid Process Using Support Vector Machines and Latent Dirichlet Allocation[C]. *2018 IEEE International Conference on Big Data*, 2018: 5008-5013.

[31] Ritter A, Wright E, Casey W, et al. Weakly Supervised Extraction of Computer Security Events from Twitter[C]. *The 24th International Conference on World Wide Web*, 2015: 896-905.

[32] Dionísio N, Alves F, Ferreira P M, et al. Cyberthreat Detection from Twitter Using Deep Neural Networks[C]. *2019 International Joint Conference on Neural Networks*, 2019: 1-8.

[33] Resource description framework. https://www.sciencedirect.com/topics/computer-science/resource-description-framework. 2017.

[34] Feng X, Liao X, Wang X, et al. Understanding and securing device vulnerabilities through automated bug report analysis[C]. *The 28th USENIX Conference on Security Symposium*, 2019: 887-903.

[35] Mu D, Cuevas A, Yang L, et al. Understanding the reproducibility of crowd-reported security vulnerabilities[C]. *27th {USENIX} Security Symposium,* 2018: 919-936.

[36] Neil L, Mittal S, Joshi A. Mining Threat Intelligence about Open-Source Projects and Libraries from Code Repository Issues and Bug Reports[C]. *2018 IEEE International Conference on Intelligence and Security Informatics*, 2018: 7-12.

[37] Github. https://github.com. 2008.

[38] Gitlab. https://about.gitlab.com/. 2013.

[39] Bitbucket. https://bitbucket.org. 2012.

[40] Husari G, Al-Shaer E, Ahmed M, et al. TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources[C]. *The 33rd Annual Computer Security Applications Conference*, 2017: 103-115.

[41] Husari G, Niu X, Chu B, et al. Using Entropy and Mutual Information to Extract Threat Actions from Cyber Threat Intelligence[C]. *2018 IEEE International Conference on Intelligence and Security Informatics*, 2018: 1-6.

[42] Ramnani R R, Shivaram K, Sengupta S, et al. Semi-Automated Information Extraction from Unstructured Threat Advisories[C]. *The 10th Innovations in Software Engineering Conference*, 2017: 181-187.

[43] Kim N, Lee S, Cho H, et al. Design of a Cyber Threat Information Collection System for Cyber Attack Correlation[C]. *2018 International Conference on Platform Technology and Service*, 2018: 1-6.

[44] Li K, Wen H, Li H, et al. Security OSIF: Toward Automatic Discovery and Analysis of Event Based Cyber Threat Intelligence[C]. *2018 IEEE SmartWorld*, *Ubiquitous Intelligence & Computing*, *Advanced & Trusted Computing*, *Scalable Computing & Communications*, *Cloud & Big Data Computing*, *Internet of People and Smart City Innovation*, 2018: 741-747.

[45] Niakanlahiji A, Safarnejad L, Harper R, et al. IoCMiner: Automatic Extraction of Indicators of Compromise from Twitter[C]. *2019 IEEE International Conference on Big Data*, 2019: 4747-4754.

[46] Syed Z, Padia A, Finin T, et al. UCO: A unified cybersecurity ontology[J]. *UMBC Student Collection*, 2016: 259-261.

[47] Thelen M, Riloff E. A Bootstrapping Method for Learning Semantic Lexicons Using Extraction Pattern Contexts[C]. *The ACL-02 conference on Empirical methods in natural language processing - EMNLP'02*, 2002: 214-221.

[48] Jo H, Kim J, Porras P, et al. GapFinder: Finding Inconsistency of Security Information from Unstructured Text[J]. *IEEE Transactions on Information Forensics and Security*, 2021, 16: 86-99.

[49] Studer R, Benjamins V R, Fensel D. Knowledge Engineering: Principles and Methods[J]. *Data & Knowledge Engineering*, 1998, 25(1/2): 161-197.

[50] Drumond L, Girardi R. A Survey of Ontology Learning Procedures[J]. *WONTO*, 2008, 427: 1-13.

[51] Dong C, Jiang B, Lu Z G, et al. Knowledge Graph for Cyberspace Security Intelligence: A Survey[J]. *Journal of Cyber Security*, 2020(5): 56-76.
(董聪, 姜波, 卢志刚, 等. 面向网络空间安全情报的知识图谱综述[J]. *信息安全学报*, 2020(5):56-76.)

[52] Zhao Y S, Lang B, Liu M. Ontology-Based Unified Model for Heterogeneous Threat Intelligence Integration and Sharing[C]. *2017 11th IEEE International Conference on Anti-counterfeiting*, *Security*, *and Identification*, 2017: 11-15.

[53] Adithya M, Dr S B. Security Analysis and Preserving Block-Level Data DE-Duplication In Cloud Storage Services[J]. *Journal of Trends in Computer Science and Smart Technology*, 2020, 2(2): 120-126.

[54] Edwards C, Migues S, Nebel R, et al. System and method of data collection, processing, analysis, and annotation for monitoring cyber-threats and the notification thereof to subscribers. U.S. Patent Application 09/950,820[P]. 2002-3-28.

[55] Brown S, Gommers J, Serrano O. From Cyber Security Information Sharing to Threat Management[C]. *The 2nd ACM Workshop*

on Information Sharing and Collaborative Security, 2015: 43-49.

[56] Modi A, Sun Z B, Panwar A, et al. Towards Automated Threat Intelligence Fusion[C]. *2016 IEEE 2nd International Conference on Collaboration and Internet Computing*, 2016: 408-416.

[57] Azevedo R, Medeiros I, Bessani A. PURE: Generating Quality Threat Intelligence by Clustering and Correlating OSINT[C]. *2019 18th IEEE International Conference on Trust, Security and Privacy In Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering*, 2019: 483-490.

[58] Sun T F, Yang P, Li M M, et al. An Automatic Generation Approach of the Cyber Threat Intelligence Records Based on Multi-Source Information Fusion[J]. *Future Internet*, 2021, 13(2): 40.

[59] Meng T, Jing X Y, Yan Z, et al. A Survey on Machine Learning for Data Fusion[J]. *Information Fusion*, 2020, 57: 115-129.

[60] Belhajem I, Maissa Y B, Tamtaoui A. Improving Vehicle Localization In a Smart City with Low Cost Sensor Networks and Support Vector Machines[J]. *Mobile Networks and Applications*, 2018, 23(4): 854-863.

[61] Alam F, Mehmood R, Katib I, et al. Data Fusion and IoT for Smart Ubiquitous Environments: A Survey[J]. *IEEE Access*, 2017, 5: 9533-9554.

[62] Bouwman X, Griffioen H, Egbers J, et al. A different cup of {TI}? The added value of commercial threat intelligence[C]. *29th {USENIX} Security Symposium*, 2020: 433-450.

[63] de Melo e Silva A, Costa Gondim J J, de Oliveira Albuquerque R, et al. A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence[J]. *Future Internet*, 2020, 12(6): 108.

[64] Li L. *Study on the Multi-Dimensional Analysis Model of Threat Intelligence Credibility In Cyberspace*[D]. Beijing: Beijing University of Posts and Telecommunications, 2018.
(李蕾. 网络空间中威胁情报可信度多维度分析模型研究[D]. 北京: 北京邮电大学, 2018.)

[65] Liu H S, Tang H Y, Bo M X, et al. A Multi-Source Threat Intelligence Confidence Value Evaluation Method Based on Machine Learning[J]. *Telecommunications Science*, 2020, 36(1): 119-126.
(刘汉生, 唐洪玉, 薄明霞, 等. 基于机器学习的多源威胁情报质量评价方法[J]. *电信科学*, 2020, 36(1): 119-126.)

[66] Li V G, Dunn M, Pearce P, et al. Reading the tea leaves: A comparative analysis of threat intelligence[C]. *28th {USENIX} Security Symposium*, 2019: 851-867.

[67] Schaberreiter T, Kupfersberger V, Rantos K, et al. A Quantitative Evaluation of Trust In the Quality of Cyber Threat Intelligence Sources[C]. *The 14th International Conference on Availability, Reliability and Security*, 2019: 1-10.

[68] Schlette D, Böhm F, Caselli M, et al. Measuring and Visualizing Cyber Threat Intelligence Quality[J]. *International Journal of Information Security*, 2021, 20(1): 21-38.

[69] Griffioen H, Booij T, Doerr C. Quality Evaluation of Cyber Threat Intelligence Feeds[C]. *International Conference on Applied Cryptography and Network Security*, 2020: 277-296.

[70] Li Q, Jiang Z W, Yang Z M, et al. A Quality Evaluation Method of Cyber Threat Intelligence In User Perspective[C]. *2018 17th IEEE International Conference on Trust, Security and Privacy In Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering*, 2018: 269-276.

[71] Al-Ibrahim O, Mohaisen A, Kamhoua C, et al. Beyond Free Riding: Quality of Indicators for Assessing Participation In Information Sharing for Threat Intelligence[EB/OL]. 2017: arXiv preprint arXiv:1702.00552.

[72] Gao Y L, Li X Y, Li J R, et al. Graph Mining-Based Trust Evaluation Mechanism with Multidimensional Features for Large-Scale Heterogeneous Threat Intelligence[C]. *2018 IEEE International Conference on Big Data*, 2018: 1272-1277.

[73] Meier R, Scherrer C, Gugelmann D, et al. FeedRank: A Tamper-Resistant Method for the Ranking of Cyber Threat Intelligence Feeds[C]. *2018 10th International Conference on Cyber Conflict*, 2018: 321-344.

[74] Cheng X L. *Study on Trustworthy Analysis of Threat Intelligence Based on Machine Learning*[D]. Beijing: Beijing University of Posts and Telecommunications, 2019.
(程翔龙. 基于机器学习的威胁情报可信分析系统的研究[D]. 北京: 北京邮电大学, 2019.)

[75] Threat Hunting Report 2017. https://www.cybereason.com/2017-threat-hunting-report. Marc. 2017.

[76] Gao P, Shao F, Liu X Y, et al. Enabling Efficient Cyber Threat Hunting with Cyber Threat Intelligence[C]. *2021 IEEE 37th International Conference on Data Engineering*, 2021: 193-204.

[77] Arnold N, Ebrahimi M, Zhang N, et al. Dark-Net Ecosystem Cyber-Threat Intelligence (CTI) Tool[C]. *2019 IEEE International Conference on Intelligence and Security Informatics*, 2019: 92-97.

[78] Gascon H, Grobauer B, Schreck T, et al. Mining Attributed Graphs for Threat Intelligence[C]. *The Seventh ACM on Conference on Data and Application Security and Privacy*, 2017: 15-22.

[79] Milajerdi S M, Eshete B, Gjomemo R, et al. POIROT: Aligning Attack Behavior with Kernel Audit Records for Cyber Threat Hunting[C]. *The 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019: 1795-1812.

[80] Kim E, Kim K, Shin D, et al. CyTIME: Cyber Threat Intelligence ManagEment Framework for Automatically Generating Security Rules[C]. *The 13th International Conference on Future Internet Technologies*, 2018: 1-5.

[81] Li D, Zhou X, Xue A. Open Source Threat Intelligence Discovery Based on Topic Detection[C]. *2020 29th International Conference on Computer Communications and Networks*, 2020: 1-4.

[82] Gao Y L, Li X Y, Peng H, et al. HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network[J]. *IEEE Transactions on Knowledge and Data Engineering*, 7019, PP(99): 1.

[83] Samtani S, Chinn K, Larson C, et al. AZSecure Hacker Assets Portal: Cyber Threat Intelligence and Malware Analysis[C]. *2016 IEEE Conference on Intelligence and Security Informatics*, 2016: 19-24.

[84] Shu X K, Araujo F, Schales D L, et al. Threat Intelligence Computing[C]. *The 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018: 1883-1898.

[85] Husari G, Al-Shaer E, Chu B, et al. Learning APT Chains from Cyber Threat Intelligence[C]. *The 6th Annual Symposium on Hot*

Topics in the Science of Security - HotSoS '19, 2019: 1-2.

[86] Li J T, Shi Y, Xue Z. APT Detection Based on DNS Traffic and Threat Intelligence[J]. *Information Security and Communications Privacy*, 2016, 14(7): 84-88.
(李骏韬, 施勇, 薛质. 基于 DNS 流量和威胁情报的 APT 检测[J]. *信息安全与通信保密*, 2016, 14(7): 84-88.)

[87] Wen S H, He N Q, Yan H B. Detecting and Predicting APT Based on the Study of Cyber Kill Chain with Hierarchical Knowledge Reasoning[C]. *The 2017 VI International Conference on Network, Communication and Computing*, 2017: 115-119.

[88] Gschwandtner M, Demetz L, Gander M, et al. Integrating Threat Intelligence to Enhance an Organization's Information Security Management[C]. *The 13th International Conference on Availability, Reliability and Security*, 2018: 1-8.

[89] Moustafa N, Adi E, Turnbull B, et al. A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems[J]. *IEEE Access*, 2018, 6: 32910-32924.

[90] Zhang H, Yi Y, Wang J, et al. Network Security Situation Awareness Framework Based on Threat Intelligence[J]. *Computers, Materials and Continua*, 2018, 56(3): 381-399.

[91] Wang J S, Yi Y Z, Zhang H B, et al. Network Attack Prediction Method Based on Threat Intelligence[M]. Cloud Computing and Security. Cham: Springer International Publishing, 2018: 151-160.

[92] Grisham J, Samtani S, Patton M, et al. Identifying Mobile Malware and Key Threat Actors In Online Hacker Forums for Proactive Cyber Threat Intelligence[C]. *2017 IEEE International Conference on Intelligence and Security Informatics*, 2017: 13-18.

[93] Bou-Harb E, Lucia W, Forti N, et al. Cyber Meets Control: A Novel Federated Approach for Resilient CPS Leveraging Real Cyber Threat Intelligence[J]. *IEEE Communications Magazine*, 2017, 55(5): 198-204.

[94] Zhang H B, Yi Y Z, Wang J S, et al. Network Attack Prediction Method Based on Threat Intelligence for IoT[J]. *Multimedia Tools and Applications*, 2019, 78(21): 30257-30270.

[95] Ranade P, Mittal S, Joshi A, et al. Using Deep Neural Networks to Translate Multi-Lingual Threat Intelligence[C]. *2018 IEEE International Conference on Intelligence and Security Informatics*, 2018: 238-243.

[96] Gandotra E, Bansal D, Sofat S. A Framework for Generating Malware Threat Intelligence[J]. *Scalable Computing*: *Practice and Experience*, 2017, 18(3): 195-206.

[97] Hu X, Jang J, Wang T, et al. Scalable Malware Classification with Multifaceted Content Features and Threat Intelligence[J]. *IBM Journal of Research and Development*, 2016, 60(4): 6: 1-6: 11.

[98] Piplai A, Mittal S, Abdelsalam M, et al. Knowledge Enrichment by Fusing Representations for Malware Threat Intelligence and Behavior[C]. *2020 IEEE International Conference on Intelligence and Security Informatics*, 2020: 1-6.

[99] Zhu Z Y, Dumitraş T. FeatureSmith: Automatically Engineering Features for Malware Detection by Mining the Security Literature[C]. *The 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016: 767-778.

[100] Wang X, Wu Y, Lu Z G. Study on Malicious URL Detection Based on Threat Intelligence Platform[J]. *Computer Science*, 2018, 45(3): 126-132, 172.
(汪鑫, 武杨, 卢志刚. 基于威胁情报平台的恶意 URL 检测研究[J]. *计算机科学*, 2018, 45(3): 126-132, 172.)

[101] Zhou Y, Wang P C. An Ensemble Learning Approach for XSS Attack Detection with Domain Knowledge and Threat Intelligence[J]. *Computers & Security*, 2019, 82: 261-269.

[102] Serketzis N, Katos V, Ilioudis C, et al. Improving Forensic Triage Efficiency through Cyber Threat Intelligence[J]. *Future Internet*, 2019, 11(7): 162.

[103] Serketzis N, Katos V, Ilioudis C, et al. Actionable Threat Intelligence for Digital Forensics Readiness[J]. *Information & Computer Security*, 2019, 27(2): 273-291.

[104] The Linux Audit Framework. https://github.com/linux-audit/. 2016.

[105] ETW events in the common language runtime. https://docs.microsoft.com/en-us/dotnet/framework/performance/etw-events-in-the-common-language-runtime. Marc. 2017.

[106] Sysdig. http://www.sysdig.org/. 2015.

[107] Vishwanathan S V N, Schraudolph N N, Kondor R, et al. Graph kernels[J]. *Journal of Machine Learning Research*, 2010, 11: 1201-1242.

[108] Sundar C, Priyanga R. Mining Words and Targets using Alignment Model[J]. *Journal of Applied Sciences Research,* 2015, 11(19): 46-49.

[109] Breneman J. Kernel Methods for Pattern Analysis[J]. *Technometrics*, 2005, 47(2): 237.

[110] SPARQL query language. http://www.w3.org/TR/rdf-sparql-query/. 2008.

[111] Wang Q X, Yang W. Extraction of Threat Intelligence Entities Based on STIX[J]. *Cyberspace Security*, 2020, 11(8): 86-91.
(王沁心, 杨望. 基于 STIX 标准的威胁情报实体抽取研究[J]. *网络空间安全*, 2020, 11(8): 86-91.)

[112] Wang X R, Xiong Z H, Du X Y, et al. NER In Threat Intelligence Domain with TSFL[C]. *CCF International Conference on Natural Language Processing and Chinese Computing*, 2020: 157-169.

[113] Yi F, Jiang B, Wang L, et al. Cybersecurity Named Entity Recognition Using Multi-Modal Ensemble Learning[J]. *IEEE Access*, 2020, 8: 63214-63224.

[114] Tundis A, Ruppert S, Mühlhäuser M. On the Automated Assessment of Open-Source Cyber Threat Intelligence Sources[C]. *International Conference on Computational Science*, 2020: 453-467.

[115] Menges F, Putz B, Pernul G. DEALER: Decentralized Incentives for Threat Intelligence Reporting and Exchange[J]. *International Journal of Information Security*, 2021, 20(5): 741-761.

[116] Yucel C, Chalkias I, Mallis D, et al. On the Assessment of Completeness and Timeliness of Actionable Cyber Threat Intelligence Artefacts[C]. *International Conference on Multimedia Communications, Services and Security*, 2020: 51-66.

[117] Wagner T D, Mahbub K, Palomar E, et al. Cyber Threat Intelligence Sharing: Survey and Research Directions[J]. *Computers & Security*, 2019, 87: 101589.

[118] Xiao Z F. Towards a Two-Phase Unsupervised System for Cybersecurity Concepts Extraction[C]. *2017 13th International Conference on Natural Computation*, *Fuzzy Systems and Knowledge*

Discovery, 2017: 2161-2168.

[119] Ampel B, Samtani S, Zhu H Y, et al. Labeling Hacker Exploits for Proactive Cyber Threat Intelligence: A Deep Transfer Learning Approach[C]. *2020 IEEE International Conference on Intelligence and Security Informatics*, 2020: 1-6.

[120] Williams R, Samtani S, Patton M, et al. Incremental hacker forum exploit collection and classification for proactive cyber threat intelligence: An exploratory study[C]. *2018 IEEE International Conference on Intelligence and Security Informatics*, 2018: 94-99.

崔琳 于 2020 年在中国传媒大学信息安全专业获得工学学士学位。现在西北工业大学网络空间安全专业攻读研究生学位。研究领域为威胁情报挖掘, 威胁情报关联分析等。Email: lincui@mail.nwpu.edu.cn

杨黎斌 于 2009 年在西北工业大学控制科学与工程专业获得博士学位。现任西北工业大学网络空间安全学院副教授。研究兴趣为物联网安全、移动网络激励, 网络信息检索等。Email: libiny@nwpu.edu.cn

何清林 现任国家互联网应急中心高级工程师。主要研究方向: 网络信息安全, 恶意样本分析, 物联网威胁情报及高级威胁研究。Email: hql@cert.org.cn

王梦涵 现在西北工业大学信息安全专业攻读工学学士学位。研究领域为网络空间安全、机器学习、自然语言处理。研究兴趣包括: 信息内容安全、威胁情报等。Email: wmh@mail.nwpu.edu.cn

马建锋 于 1995 年在西安电子科技大学通信与电子系统专业获得工学博士学位。现任西安电子科技大学教授。研究领域为网络空间安全。研究兴趣包括: 应用密码学、无线网络安全、数据安全、移动智能系统安全。Email: jfma@mail.xidian.edu.cn