刘金,秦媛媛,田晓娜,等. 开源网络威胁情报技术研究综述[J]. 智能计算机与应用,2024,14(11):24-34. DOI:10.20169/j.issn.2095-2163.241104

开源网络威胁情报技术研究综述

刘 金, 秦媛媛, 田晓娜, 郝 娇, 韩庆敏
(华北计算机系统工程研究所, 北京 100083)

摘 要: 随着互联网络的快速发展,新型网络安全威胁也在不断演变。传统的被动流量监测方式,难以满足网络安全防护全部要求。在发生网络攻击之前,提前获取威胁情报可以更有效地应对安全威胁,避免财产损失。开源网络威胁数据获取成本低、收益高的特点,使其成为威胁情报的重要来源之一。大数据、人工智能、区块链等新技术,为开源网络威胁情报获取、分析及共享提供了重要手段。本文分析了国内外开源网络威胁情报研究进展及各项技术在开源网络威胁情报处理分析共享过程中的应用,总结了共性问题和未来趋势。

关键词: 开源情报; 网络威胁情报; 大数据; 人工智能; 区块链
中图分类号: TP393 **文献标志码**: A **文章编号**: 2095-2163(2024)11-0024-11

A review of open source cyber threat intelligence technology research

LIU Jin, QIN Yuanyuan, TIAN Xiaona, HAO Jiao, HAN Qingmin
(National Computer System Engineering Research Institute of China, Beijing 100083, China)

Abstract: With the rapid development of Internet, new types of cyber security threats are constantly evolving . The traditional passive traffic monitoring methods cannot meet all the requirements of cyber security protection. Obtaining threat intelligence in advance before cyber attacks can deal with security threats more effectively and avoid property losses. The low cost and high profit of obtaining open source cyber threat intelligence make it become one of the important sources of threat intelligence. New technologies such as big data, artificial intelligence and blockchain provide important methods for obtaining, analyzing and sharing open source cyber threat intelligence. This paper analyzes the research progress of open source cyber threat intelligence at home and abroad and the application of various technologies in the process of open source cyber threat intelligence processing, analysis and sharing and summarizes the common problems and future trends.

Key words: open source intelligence; cyber threat intelligence; big data; Artificial Intelligence; blockchain

0 引 言

随着互联网的快速发展及“万物互联”时代的到来,网络空间已成为继陆、海、空、天后的“第五空间”[1],APT 攻击、DDoS 攻击等网络安全威胁也愈加复杂多变。依靠传统被动流量监测方式,难以实现全面防护。针对网络空间不断变更的新型威胁,提前获取网络攻击者的攻击方式、攻击意图等威胁情报信息,有助于推动网络安全事件的快速响应,减轻安全风险。

当前网络威胁情报信息(Cyber threat intelligence, CTI)的来源,不仅仅依赖于专业的网络安全厂商以产品形式分享的商业威胁情报,更多地来源于攻击方、网络安全爱好者、网络安全专家在公开网络、广播、新闻采访及社交媒体平台分享的开源情报信息[2]。鉴于开源情报低风险、低成本、高收益的特点,已成为获取威胁情报信息的主要途径。而随着开源网络威胁情报数据日益增加,数据量及更新频次不断增长,数据信息呈现数据量大(Volume)、数据更新快(Velocity)、数据种类多样(Variety)、数据黏度大(Viscosity)、数据波动大(Volatility)等特点[3]。依靠单一系统获取的数据进行分析,难以满足应用的全部需求,依靠新兴技术搭建数据共享平台,交换获取的数据信息,增强对组织内网络威胁和

作者简介: 刘 金(1990—),女,工程师,主要研究方向:工控安全,网络安全; 秦媛媛(1987—),女,高级工程师,主要研究方向:信息安全,网络靶场; 田晓娜(1989—),女,工程师,主要研究方向:信息安全,网络靶场。
通信作者: 韩庆敏(1979—),女,正高级工程师,主要研究方向:网络安全,工控安全。Email:hanqm@ncse.com.cn。

收稿日期: 2023-06-25

违反政策行为的可见性，通过进行协作，积极保护其系统和网络免受网络攻击，是有效利用数据，提升网络安全应对能力的重要途径之一。而新兴技术应用于数据的收集与共享，亦可能导致安全问题，使得网络威胁制造者同样获取系统脆弱性、漏洞信息，利用相应信息达到恶意目的，如利用数据集训练攻击模型，增强攻击能力，更有针对性地发动网络攻击等[4]。如何平衡信息新兴技术和数据安全之间的关系，是学术界面临的一个长期问题。本文对国内外开源网络威胁情报研究进展及技术进行了梳理，总结了当前主流技术热点，归纳了共性问题，展望了未来趋势与挑战。

1　基本概念

1.1　开源情报

开源情报指基于某种目的对公开来源数据进行收集和处理，而得到的某种显式或隐含的信息。随着 21 世纪互联网的发展，大量信息溢出，社交媒体开辟了新的视角，提供了新的数据和元数据类别，允许在任何层面对实体或群体进行微观分析和剖析[5-6]。移动数据访问设备的出现则使这一趋势进一步加强，进而导致社交媒体的使用频率显著增加[6]。新技术满足了情报部门管理大量数据的需求，推进了情报周期的具体活动，特别是在信息的收集、处理、管理和传播方面。开源情报的重要性迅速显现，公司和用户可以根据其目的的不同，使用不同的开源情报工具并收集数据[7]。

从互联网络海量开源数据到通过分析关联，归纳总结出有效的开源情报，在处理过程中，会产生不同种类的数据信息，如图 1 所示[8]。

图 1　开源情报处理[8]

Fig. 1　Process of open source intelligence[8]

由图 1 可知，首先从公开渠道获取的文本、图像、音频、视频、元数据等开源数据；根据某些要求或标准进行过滤，生成了主题书籍、文章、论文等开源信息；针对开源信息中，为满足特定目的，经过检索和过滤等流程处理后的数据，数据信息被汇总、分类，并且可以输送给互相关开源情报工具，形成开源情报（Open-source intelligence，OSINT）；判断信息来源可验证，未被恶意用户篡改传播具有高度确定性/准确性的 OSINT 可以成为有效的开源情报。

在网络安全领域，OSINT 收集的数据在安全方面得到正确使用，就可以提前预防可能在网络空间发生的网络犯罪、网络安全威胁和网络恐怖活动[4]。使用 OSINT 来应对网络攻击的研究仍在推进中[9]。

1.2　网络威胁情报

2013 年 5 月，Gartner 首次提出网络威胁情报的概念[10]：某种现有或即将出现的基于证据的网络资产的威胁知识，包括场景、机制、指标、启示和可操作建议等，且这些知识可为主体提供威胁的应对策略。

网络威胁情报分层展示如图 2 所示。情报获取难度、稳定性、信息量从下到上逐渐增强[11]。

图 2　网络威胁情报分层展示[11]

Fig. 2　The layers of cyber threat intelligence[11]

主要情报内容包括：失陷指标（Indicators of Compromise，IoC），如文件的 HASH、程序运行路径、注册表项、攻击者的 IP 地址、域名、URL 等相关标签，通过什么动作执行来达成战术的目标；主要指战术、技术和程序（Tactics、Techniques、Procedures，TTP），包括对攻击行动的概括性要求、目的或行动原因；事件相关组织及人员等。

通常，网络威胁情报生命周期如图 3 所示[12]。

图 3　网络威胁情报生命周期[12]

Fig. 3　Cyber threat intelligence lifecycle[12]

在规划过程中明确要保护的资产和业务，评估受到破坏的潜在影响，明晰情报获取的需求与期望达到的目标，规划数据的收集；根据规划收集内部（日志、事件）和外部资源（安全公告、安全报告、论文、社交媒体言论、匿名网络数据等）的威胁数据；将收集的数据进行翻译，聚合等操作后，对情报内容

进行识别与关联,评估情报的质量,确认是否满足要求。当前较为成熟的威胁情报分析模型,如 Cyber Kill Chain[13],ATT&CK[14] 等模型,可将原始数据转换成真正具有重要意义的情报,找到其真正的价值,将数据收集与情报区分开来;将有价值的情报进行传播,目前已定义的标准化分享格式包括 STIX[15]、TAXII[16] 或 CybOX[17] 等等;根据共享情况实施反馈,判断是否需要重新通过“规划”进行调整。

2 开源网络威胁情报处理与共享

2.1 开源网络威胁情报的基本架构

根据网络威胁情报生命周期和 ISO/IEC 27037:2012[18-19] 和 ISO/IEC 27042:2015[18-20] 等数字取证阶段,总结开源网络威胁情报平台基础框架如图 4 所示。首先识别收集有效范围,包括有效的新闻网站、社交媒体、匿名网络、论文报告等。通过工具针对相应网站、社交媒体进行数据获取;获取到相应数据后,对数据进行分类,结合已有的网络威胁数据库,对数据进行缓存处理;数据集成处理过程是对数据进行抽取及规范化处理,对位置、攻击者、漏洞、攻击方式、恶意软件等实体加以识别,并进行实体间关系识别等,调用数据集成工具,按步骤进行数据处理;在数据分析阶段,应用各种算法分析工具,对处理后的数据进行关联分析,依据分析结果,报告网络威胁,在分析阶段旨在实现 3 个目标:空间意识、情境意识和一些尝试性预测[21];在数据获取、处理和分析过程中,可通过人机交互界面查看相应结果,如果发现偏差,可进行人为纠正。

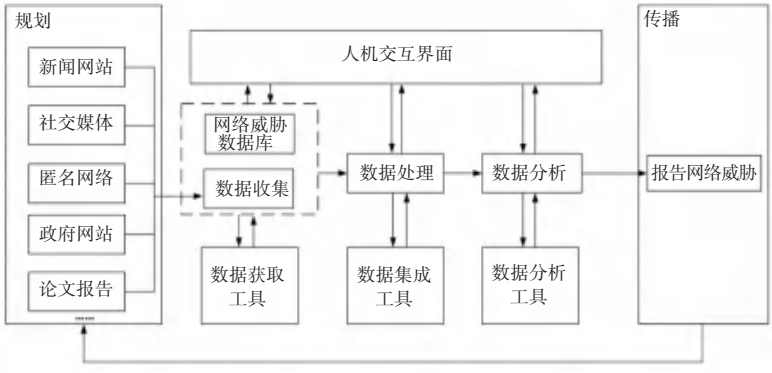

图 4 开源网络威胁情报平台基础框架

Fig. 4 Basic framework of open source cyber threat intelligence platform

在对情报数据进行规划时,根据情报类别确认获取来源,常见分类主要包括战略威胁情报、运营威胁情报、战术威胁情报、技术威胁情报等。其中,战略情报指与威胁格局相关的高级情报[22],其受众为企业高层和董事会人员。由非技术性数据组成,如风险信息和用于长期战略的业务目标,根据这些知识对预算进行优先排序。这些信息通常来自国家或地方媒体、研究报告和行业特定出版物[23]。运营情报的目标是检测针对组织的特定威胁[24]。这些信息可能是从封闭的论坛或匿名网络收集的,目的是检测可能表明组织未来受到攻击的提示,这些信息很难收集且很少被发现,但从漏洞管理的角度来看,运营情报是非常宝贵的,提供了实时的利用信息,有助于确定漏洞修补的优先级[25]。战术情报的目标是收集有关威胁行为者战术、技术和程序(TTP)的信息[24]。通过战术情报,可以了解攻击者的行为方式以及常见使用的工具。这种威胁分析提供了对手如何进行攻击的见解,这可以帮助相关从业人员做出应对[26]。技术情报是特定攻击的信息,可以从威胁行为者的行为、内部日志和妥协指标(IoC)中收集到的此类情报[25],可以加快数据分类并提高可见性,常被用于检测和补救[25]。

2.2 数据安全控制与隐私保护要求

目前,对于如何收集、分析和获取社交媒体等公开来源的威胁情报信息,没有国家或国际公认的指导方针[27]。默认的守则是:从社交媒体等公开来源收集的情报必须以不违反现有隐私法的方式进行,不得以恶意方式使用,且仅在必要时进行[28]。基于隐私的设计(Privacy by Design,PbD)以及数据保护的主要概念已经在计算机科学和法律研究界广泛传播,为了平衡开源情报与个人隐私问题,欧洲启动了 CAPER 项目,旨在建立一个以预防组织犯罪为目标的 OSINT 解决方案,来平衡自由与安全。Casanovas[29] 依靠语义网络管理模型(SWRM)的隐私设计(PbD)原则,将欧洲通用数据改革方案(GDRP)的欧洲的法律和伦理问题嵌入到 CAPER

监控平台，通过制度设计、自监管讨论，提出了建立法治的可能性。Ghioni 等学者[30]分析了与治理、伦理、法律和社会（GELSI）框架相关的人工智能 OSINT 的使用，以及 OSINT 软件的开发文献的现状，强调了潜在的差距，并提出了新的研究方向。

有效的数据安全和隐私策略，可以避免非法用户对数据的恶意的访问及利用，符合利益相关方的需求及组织的最高利益[3]。美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）定义数据安全控制指在系统或组织内使用的保障措施或对策，以保护系统及其数据的机密性、完整性和可用性，并管理信息安全风险。隐私控制是在系统或组织中使用的管理、技术和物理保障，以管理隐私风险，并确保遵守适用的隐私要求[31]。

在数据安全方面，保护数据的机密性，可以防止数据泄露及未经授权的访问与滥用[3]，如：实施访问控制措施，确保只有获得授权的用户才能访问相关数据；采用加密手段进行敏感数据脱敏，即使发生数据泄露，没有解密密钥，数据仍然不可读；建立安全监控审计机制，监控数据访问和使用情况等等。保护数据的完整性，防止未经授权的数据修改或损坏并提高数据质量，如：检测数据是否在传输或存储过程中被篡改或损坏；对数据进行备份防止数据丢失，在问题发生时保证数据可恢复；设置访问控制机制，限制对数据的操作限等等。保护数据的可用性，确保数据在需要时可被及时访问、使用和传输，保证业务的连续性和数据的可靠性。如采用冗余存储，在一个存储设备发生故障时，仍然可以从其他设备上获取数据；合理容量规划和资源管理，避免因为资源不足而导致数据无法及时访问和使用；使用监控工具和警报系统来实时监测系统和数据的状态，及时发现潜在的故障、错误或性能问题，并采取相应措施，以确保数据的持续可用性；部署适当的安全设备，保护系统免受安全威胁和恶意攻击等等。对数据进行安全风险评估，了解面临的安全威胁，降低组织面临的信息安全风险；制定和实施适当的安全政策、规范和流程，明确组织对信息安全的要求和期望；建立风险治理框架，确定责任和权限，确保风险管理活动得到适当的管理和监督；开展定期的安全培训和意识提升活动，向员工传达信息安全的重要性，并提供实际操作的安全指导等等。

对数据进行隐私控制，可以确保数据的合法、安全和适当使用，如：根据数据的敏感性和隐私级别进行分类和标记，确保对不同级别的数据采取适当的保护措施；只收集、使用和保留必要的个人数据，避免收集不必要或过多的数据；确保个人数据的处理符合适用的隐私法律和法规，包括获取合法授权、明确目的和合规数据处理流程等等。在法律法规方面，欧盟于 2016 年通过了数据保护和隐私法规 Regulation（EU）2016/679《通用数据保护条例》（General Data Protection Regulation，GDPR）。中国于 2021 年开始实施《数据安全保护法》及《个人信息保护法》。美国于 2022 年发布了《美国数据隐私和保护法》（American Data Privacy and Protection Act，ADPPA），加强对个人数据的保护，促进数据的合法、透明和负责任的处理，以维护个人隐私。

2.3　网络威胁情报共享战略与技术

随着技术的发展，未知威胁和事件指标的数量不断增加，现有解决方案中的威胁分类难以覆盖全部威胁信息，依靠单独机构或选定的用户间进行信息的分发，对威胁检测和处理带来一系列限制。Dandurand 等学者[32]解释道，成功的威胁情报系统最重要的要求是共享信息的设施、自动化信息共享以及生成、定义和控制数据的能力。

在战略层面，美国已形成完善的情报机构和情报体系，NIST Special Publication 800-150[33]中描述网络威胁信息共享时，主要考虑以下几个方面：首先建立支持业务流程和安全策略的信息共享目标；识别网络威胁信息的来源；指定信息共享活动的范围；建立信息共享规则；加入并参与信息共享工作；积极寻求通过提供额外的背景、更正或建议的改进来丰富指标；使用安全、自动化的工作流程来发布、使用、分析网络威胁信息并对其采取行动；积极建立网络威胁共享协议；保护敏感信息的安全和隐私；为信息共享活动提供持续支持。其于 2015 年 2 月在情报总监办公室（ONDI）下专门设立了网络威胁情报整合中心（CTIIC），大力整合各政府机构相关部门情报信息，协作联动形成了政府层面、国家层面应对网络威胁的共享机制[34]。同时大力加强了国际合作，如 2016 年 6 月与以色列签署了双边网络威胁共享计划协议，加强威胁信息的共享；2016 年 12 月，与澳大利亚、日本签署三方信息共享协议[35]，并开展大规模网络演习检验国际共享成效。欧盟 2013 年提出了欧洲联盟的网络安全战略，阐述了欧盟关于如何最好地预防和应对网络破坏和攻击的方法，并强调网络领域的基本权利、民主和法治需要得到保护。在情报共享方面，欧盟通过多角度确立了网络威胁情报共享的战略地位，

构建了网络安全相关组织体系、战略文件与法律法规体系、信息技术保障、网络安全共享合作实践、网络安全文化为核心的战略体系框架[36]。基于多层安全治理模式,形成了欧盟主导、成员国主建、民间参与及执行机构统筹协调的网络威胁情报共享发展模式[37]。如设计了其预警系统概念数据库 E-EWS,欧洲网络安全中心网络和创新与运营能力中心(ECHO)成员可以近乎实时地协调和共享信息,并对网络敏感信息和相关数据可进行完全独立管理[38]。在技术层面,为了共享信息,通过引入不同类型的数据格式和传输机制,已经在构建信息方面投入了大量精力。例如,Barnum[39]引入了 STIX/TAXII 来组合人机数据以共享信息。Danyliw 等学者[40]在事件对象描述交换格式中,描述了 IODEF,通过将文本与结构化数据相结合,为计算机安全事件小组提供了一个数据共享框架[38]。

根据当前已有的共享方式,可建立国际合作的共享模型如图 5 所示[38]。

识别网络威胁流量及威胁情报等内容,相关行业公司获取相关信息后,依据标准及要求,上报行业相关单位,相关单位上报上级主管部门,主管部门上报给网络安全相关部门,之后进行国际共享,在进行共享的各个层级及阶段,充分考虑各项政策要求。

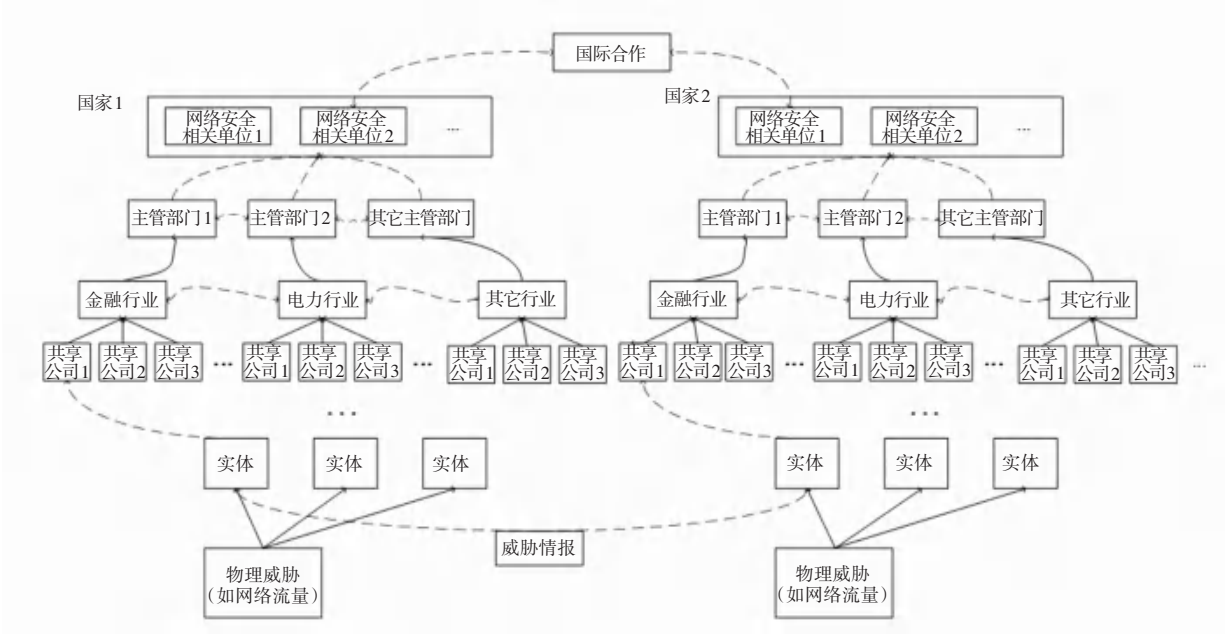

图 5 威胁情报共享模型[38]

Fig. 5 Threat intelligence sharing model[38]

3 新技术的应用

美国研究员 Williams 和 Blum[12]总结了开源情报各阶段主要新技术,Gabriel-Traian UNGUREANU 将新技术在情报各阶段生命周期进行了运用总结[41],将开源数据转变为有效的开源情报过程中,使用的技术及其作用,见表 1。

表 1 高新技术描述及作用

Table 1 Description and role of new technologies

序号	技术名称	描述及作用
1	大数据	利用大数据技术可以从许多资源中收集海量的数据,利用信息、可视化趋势,来分析过去事件原因、保持当前状态、预测未来发展趋势的一系列技术,提供了使用内部和外部安全数据来检测先进的网络攻击的机会
2	人工智能	利用人工智能技术进行分析,可为预测分析提供了深入的分析见解,自动进行数据处理,使数据分析达到更高的水平
3	区块链	利用区块链的账户匿名性可以保护威胁情报共享方和利用方的身份信息。利用区块链技术构建威胁情报信息可以实现威胁情报的共享和评级,及时、高效地获取威胁情报进行防护响应

3.1　大数据在开源网络威胁情报中的应用

对于开源网络威胁情报的大数据处理过程如图 6 所示。基于大数据技术进行网络威胁情报分析，可以从多源异构数据中快速获得有价值信息，揭示出重点内容及其变化和趋势，成为学术领域关注的热点。如 Apache Spark，为大型数据集上的分布式或联合机器学习提供了解决方案。中国信息通信研究院发布的《大数据白皮书（2016 年）》指出大数据是新资源、新技术、新理念的混合体[42]，定义了一种全新的思维角度：数据驱动与数据闭环。

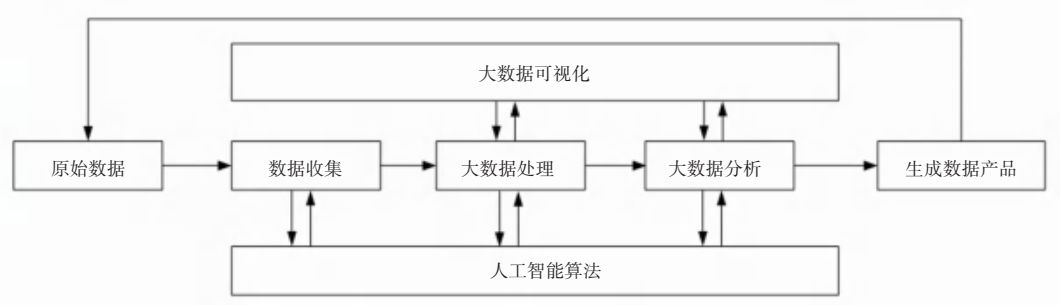

图 6　大数据处理过程

Fig. 6　Process of big data processing

伯克利大学 AMP 实验室，从大数据计算模式的角度，将大数据处理技术分为 3 种类型[43]：批量数据处理技术、流式数据处理技术、交互式数据查询分析技术。其中，批量数据处理技术通常先进行数据存储，再对存储的数据集中进行计算，来实现大量的数据吞吐。流式数据处理技术将数据移动到内存中进行实时计算，数据处理延迟短，结果实时性强。交互式数据查询分析技术常用于将人的认知能力应用到安全分析过程中[44]。基于 NoSQL 类型的数据存储，构建相应的数据索引，如根据发现的异常主体，寻找和跟踪时序变化相似的主体[45]。与非交互式数据处理相比，交互式数据处理更易于控制，是实现网络安全与情报交互式分析的关键技术之一。Nainggolan[46] 总结了 3 种技术的主要区别，见表 2。

表 2　大数据处理技术比较[46]

Table 2　Comparison of big data processing technologies[46]

	处理时间	数据量级	典型架构	应用范围[47]
批量数据处理技术	分钟到小时	TB 到 PB	Hadoop； Apache Spark	日志分析 欺诈检测 APT 检测
流式数据处理技术	连续处理	数据流	Twitter Storm； Apache Spark Streaming； Kafka	查看趋势 变动响应 查看峰值 及时性要求
交互式数据查询分析技术	毫秒到分钟	GB 到 PB	Drill Shark； Impala； Hbase	交互式分析

大数据分析是大数据环境下威胁情报安全事件关联、用户行为分析的核心，主要分为回归和机器学习技术。其中，回归技术通过在某些情况下应用各种变量之间的相互作用模型，形成数学方程构建回归模型，如线性回归模型、离散选择模型、逻辑回归模型、多项式逻辑回归模型、阶位回归模型、Logit 与 Probit 模型、时间序列模型、生存或持续时间分析、分类和回归树（CART）和多元自适应回归样条（MARS）。机器学习是人工智能技术的一个分支，使计算机能够学习处理用于回归和分类的高级统计方法的数量，在无需定义复杂状态下可能形成的变量之间的基本关系的某些情况下，这种技术可以直接预测因变量，并且相关性的数学计算未知，常见的机器学习方法包括：神经网络（NN）、多层感知器（MLP）、径向基函数、支持向量机、朴素贝叶斯、k 近邻（KNN）和地理空间预测建模等。

大数据可视化以直观的方式,帮助网络安全从业者快速发现数据背后隐含信息和知识,感知网络安全问题。可视化采用雷达图、时空图、频次图、GIS地图等图形,多视图关联动态协同[47-48]、大规模知识图谱与图形数据处理等技术。辅助网络安全从业者分析海量多源异构的网络安全数据,并实时做出决策,及时发现大数据中隐含的安全问题。

在互联网、物联网等丰富生态下,软件复杂度逐渐增加,带来的未知漏洞形态多样。大数据挖掘可基于安全规则进行未知威胁检测,王智民等学者[49]总结了大数据检测中的应用:基于大量的非结构化数据如安全事件日志,采用数据挖掘算法提取规则将流量或日志与提取的规则进行比对,根据比对结果达到检测入侵威胁的目的。王一丰等学者[50]从数据角度出发,总结和比较了当前针对未知网络威胁检测的几类方法,详细分析并阐述了其使用的数据、方法及适用场景。

3.2 人工智能在威胁情报中的应用

人工智能在网络安全领域的应用始于 20 世纪 80 年代中后期,随后即集中应用于基于规则的异常检测系统上,2000 年后大数据的兴起推动了人工智能的重大变化。随着技术变得越来越先进,机器学习算法成为威胁检测的强大工具。2000 年末,监督学习算法为更准确的威胁检测和预防提供了新的方法,无监督学习算法随后为异常模式识别和未知威胁识别提供了重要手段。深度学习则凭借其处理海量数据和揭示复杂模式的能力,彻底改变了网络安全局势。自然语言处理(NLP)技术的应用,也进一步增强了对文本数据的分析和对社会工程攻击的检测。

人工智能在开源网络威胁情报中有非常多的应用,如开发用于 OSINT 收集的高效数据挖掘技术,创建用于社交媒体智能的 OSINT 平台、优化实体排名和识别的 NLP 算法、或使用深度学习模型从 OSINT 数据中进行网络威胁分类,每种研究具有共同的应用性质,致力于从 OSINT 周期每个阶段出现的问题中寻找算法解决方案。机器学习和自然语言处理在 Web2.0 向 Web3.0 时代转变时,已经广泛用于智能目的的数据排序、翻译和分析方法的效率的提升,占据主导地位[51]。

人工智能的应用需要对存入数据库的开源数据进行内容、位置、空间、标签等特征提取,选择合适的特征,应用相关算法进行数据分析,在数据分析过程中,对模型进行反复训练调优,并对模型做出评价,应用过程如图 7 所示[51]。

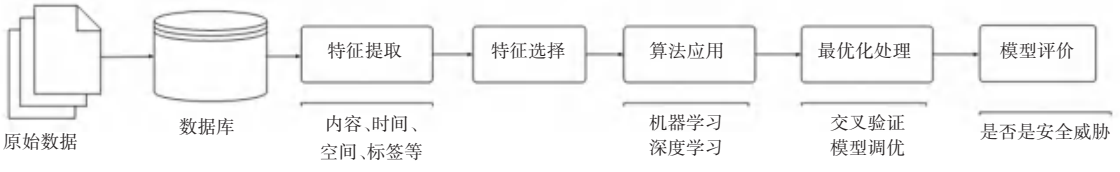

图 7 人工智能算法的应用[51]

Fig. 7 Application methods of Artificial Intelligence[51]

作为“人工智能”(AI)的核心部分,机器学习可以在从数据中发现见解方面发挥至关重要的作用。机器学习可以显著改变网络安全格局,数据科学正在引领一种新的科学范式[51-53]。机器学习和深度学习领域的最新进展和成功是在网络安全解决方案中采用人工智能技术的关键驱动因素,在管理和应对网络威胁的数字证据时提供了提高安全情报有效性的能力,应用过程如图 8 所示[54]。

但机器学习和深度学习模型也不能避免出错,总有可能检测到非真正的安全威胁,或将良性事件错误地归类为恶意事件。Arp 等学者[55]讨论了 10 个微妙的陷阱,这些陷阱破坏了机器学习模型的性能,使其可能不适合安全用例。其中一些陷阱包括抽样偏差、标签不准确、基本比率谬误和仅实验室评估。

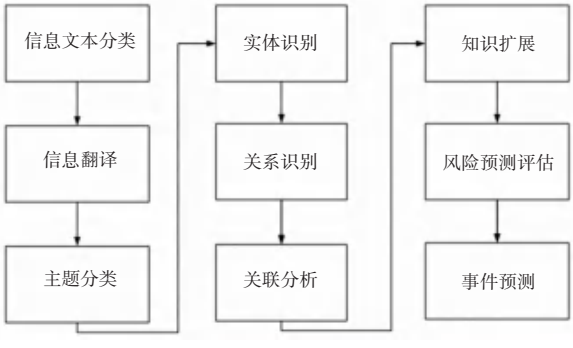

图 8 机器学习的应用过程[54]

Fig. 8 Application process of machine learning[54]

为快速自动从获取的多源信息中抽取 IOC 实体及其关系,构建结构化信息,Dionísio 等学者[56]结合 2 个自然语言处理任务的多任务学习方法,用于网络威胁情报,能够读取来自一组 Twitter 账户的推

文信息，并通过共享的深度神经网络架构，识别相关的网络安全相关内容，同时提取其中的威胁指标，在不影响功能的前提下简化了流水线以及随着时间的推移对数据和在线模型适应的要求。孙天放[57]提出了一种基于神经网络模型的威胁情报信息抽取方法（TIIE），在实体识别方面，采用长短时记忆神经网络（LSTM）实现命名实体识别，同时利用条件随机场（CRF）模型完成序列标签的约束；在关系识别方面，采用长短时记忆神经网络模型和最短依赖路径（SDP）方法进行关系抽取，提升了在进行较少特征工程研发的情况下识别的准确率、召回率和 $F-1$ 值。王淮等学者[58]通过分析网络威胁情报的特点，设计了一种实现关联分析和追踪溯源的网络威胁情报知识图谱，包括 IP、域名、样本、URL、组织和技术共 6 个实体及 14 种实体关系，以此为基础，提出 5 种关联分析算法，利用网络威胁情报关联分析技术对真实的网络威胁情报数据进行分析关联分析。罗琴等学者[59]引入主动学习方法，提出了一种结合主动学习的威胁情报 IOC 识别方法（IOC Identification Combined with Active Learning，IoC ICAL），自动化确定初始样本集大小和选取范围，对未标注数据进行伪标注实现初始样本集的有效扩展。针对威胁情报领域数据特点，通过设置样本信息熵阈值，有效获取高不确定性样本，设置样本更新量阈值作为终止条件，及时停止迭代标注，避免后续低效标注。

为解决多源网络威胁情报数据价值密度低、重复度高、失效时间快等问题，刘汉生等学者[60]提出一种基于机器学习的多源威胁情报质量评价方法，通过情报标准化和相似度匹配算法对海量情报数据进行标准化预处理，从情报来源、情报内容、活跃周期、黑名单库匹配程度共 4 个维度提取特征作为评估情报质量的依据。针对提取的特征编码，结合深度神经网络和 Softmax 分类器训练优化情报评价模型。

为提高情报分析的准确性、促进共享及使用，陈剑锋[61]针对人机协同分析策略进行研究，将人机合作的类型划分为“机器优先”“人类辅助机器”“机器辅助人类”“人类优先”共 4 个象限，开展不同的工作优化策略，并对每一象限的人机工作优化策略进行阐述和分析。

人工智能技术的操作对用户来说往往是不透明的，也不能解释具体是如何得出生成的结果的，例如，神经网络被称为“黑匣子”人工智能技术。为让用户和开发人员更容易理解人工智能算法的操作，可解释人工智能（eXplainable Artificial Intelligence，XAI）应运而生，Suryotrisongko 等学者[62]将 4 种 XAI 技术与开源智能（OSINT）混合在一起，以提供更好的解释能力。这些技术包括 AN-CHOR、LIME、SHAP 和反事实解释，并应用于入侵检测领域生成算法（DGA）类别。

从自然语言网络威胁情报（CTI）报告中提取机器可读攻击行为图的技术，依赖于一个突出的 CTI 来源，如备受瞩目的高级持续威胁（APT）报告。Olajide 提出了一种名为 CYTAG 的系统攻击行为图聚合方法[63]，该方法在给定攻击（如 APT）具有多个 CTI 源的情况下，增强了攻击图的保真度。通过攻击行为图提取和攻击行为图聚合操作，在保持攻击语义的基础上，最大限度地减少聚合攻击图中节点和边的冗余。

3.3　区块链技术在开源网络威胁情报中的应用

区块链技术作为加密货币底层技术基础[64]，具有开放、共识、去中心化、信息不可篡改、信任、可追溯等特性，将区块链技术应用于开源网络威胁情报共享中，可以减少传统中心化数据存储的单点失效问题，同时区块链信息具有信息上传者的数字签名，可以实现分享者的隐私保护和信息追溯，为分享者和利用者双方提供无需第三方监管的可信生态体系。

为平衡威胁情报共享中的隐私保护与构建完整攻击链的需求，黄克振等学者[65]提出了一种基于区块链的网络威胁情报共享模型，利用区块链的账户匿名性和信息不可篡改性，依靠单向加密函数保护共享方和利用方隐私信息，基于已加密后的情报构建完整攻击链，并借助区块链的回溯能力完成攻击链中威胁源的解密工作，发出预警。为解决单链威胁情报共享时查询性能瓶颈，提高共享意愿与共享效率，冯景瑜等学者[66]设计了情报链、监管链和积分链的多链模型，为防止内部成员恶意利用情报，并在多链模型基础上，提出跨区块链交互的威胁情报共享方案，采用哈希锁定的跨链机制来构建智能合约，确保多链间信息一致性。

为解决网络威胁情报数据共享过程中信息被恶意篡改及平台信任等问题，姜鑫等学者[67]将联盟区块链应用于网络威胁情报共享平台的搭建，对加入区块链网络内的节点进行身份认证，认证通过后，才被允许进入区块链网络，同时为准许进入网络内的节点设置权限，仅可信任节点可以参与到区块链中的共识过程当中，选择共识算法主节点时，选用高权

限的权威节点来担任。

为解决威胁情报在收集过程中出现的质量参差不齐、价值不高、容易过期等问题,史慧洋等学者[68]通过评估共享数据,建立了基于区块链和神经网络的威胁情报评估体系,实现了所选的评估指标的可计算化,达到信誉评分的动态调整,保护了用户的隐私性,同时对于恶意用户也制定了相应的惩罚措施。程叶霞等学者[69]利用区块链技术构建威胁情报信息以及威胁情报源的可信度、贡献率的区块链,设计了一种基于区块链的威胁情报共享及评级系统和一种基于区块链的威胁情报共享及评级方法,实现威胁情报的共享和评级,及时、高效地获取威胁情报进行防护响应。

区块链的应用示例如图 9 所示[70]。

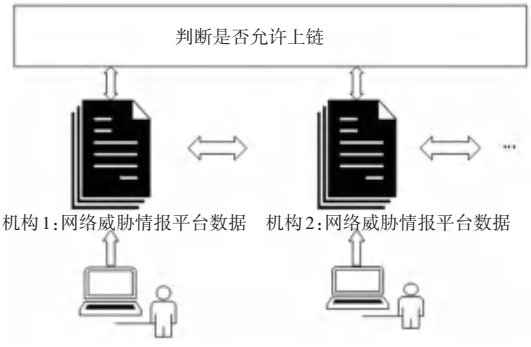

图 9 区块链的应用示例[70]

Fig. 9 Application example of blockchain[70]

4 存在问题及未来趋势

目前,很多人工智能算法模型,都是基于过去数据训练,其及时性、准确性、新的应用场景的适应性有待继续提高,依然需要网络安全从业者通过人工方式进行判断并推动数据处理及分析工作。

以 ChatGPT 为代表的生成式 AI 的出现,推动了 AI 范式的转变,其影响已初步显现,从信息的检索方式来看,对历史数据的检索更趋便捷,从分散检索向问答式检索进行转变,然而 ChatGPT 的训练具有滞后性,无法保证其提供的数据准确性,模型不具备可解释性。此外,针对生成式 AI 等高新技术,尚未有相关政策来进行全面的约束,如何平衡技术和数据安全问题,对此仍然需要更深入的探索与研究。

在数据安全指控与隐私保护方面,公众广泛采用加密技术会阻碍数据收集,并根据当地法律引发一些争议问题。如何在保证数据安全的同时,加强合作,进一步推动各个层级的开源网络威胁情报共享,共同抵抗网络威胁将成为发展趋势。

5 结束语

网络威胁情报为网络安全防护提供了重要支撑,大数据、人工智能、区块链等新技术的应用,为开源情报的获取、分析及报告,提供了重要手段。增加了网络威胁情报获取及时性,解决了情报价值随时间降低[71]的问题,而使用人工智能等快速进行数据获取,可能使得收集方法模糊、信息缺失,无法确认威胁情报准确性,可能会误报而造成附带损害,如何平衡威胁情报的及时性和准确性,仍是一个亟待解决的热点问题;同时,目前尚缺乏威胁情报采集共享和利用规范,在保护敏感信息的同时,在组织间建立信任,进一步对共享信息并实施政策、程序和技术加强管控,也包括采取积极举措施有效降低敏感信息泄露的风险,仍需后续尽快完善解决。网络空间在不断发展,研究的结论和展开的工作往往与其进行的时间段相关,可能会短暂超出从业者的能力范围[72]。

参考文献

[1] 尹丽波,刘京娟. 新形势下网络信息安全工作思考[J]. 中国信息化, 2014(9):20-22.

[2] 崔琳,杨黎斌,何清林,等. 基于开源信息平台的威胁情报挖掘综述[J]. 信息安全学报,2022,7(1):1-26.

[3] 数据管理协会(DAMA 国际). DAMA 数据管理知识体系指南[M]. 北京:机械工业出版社,2020.

[4] HWANG Y W, LEE I Y, KIM H, et al. Current status and security trend of OSINT [J]. Wireless Communications and Mobile Computing, 2022, 2022:1290129.

[5] MILLER D T. Defense 2045: Assessing the future security environment and implications for defense policymakers [M]. USA:Rowman & Littlefield, 2015.

[6] UNGUREANU G T. Open-source intelligence (OSINT). The way ahead [J]. Journal of Defense Resources Management (JoDRM), 2021, 12(1): 177-200.

[7] HAYDEN M E. Guide to Open Source Intelligence (OSINT)[EB/OL]. [2023-06-01]. https://api. semanticscholar. org/CorpusID:213320773.

[8] MILLER B H. Open source intelligence (OSINT): An oxymoron? [J]. International Journal of Intelligence and Counter Intelligence, 2018, 31(4): 702-719.

[9] WELLS D. Taking stock of subjective narratives surrounding modern OSINT[M]//AKHGAR B, BAYERL P, SAMPSON F. Open Source Intelligence Investigation. Adanced Sciences and Technologies for Security Applications. Cham: Springer, 2016: 57-65.

[10] MCMILLAN R. Definition: Threat intelligence [EB/OL]. [2018-07-12]. https:// Gartner. com.

[11] 孙铭鸿,蔡蓓蓓. 基于情报、威胁框架等方式追踪溯源方法研究[J]. 江苏通信,2022,38(3):109-112,117.

[12] WILLIAMS H J, BLUM I. Defining second generation open

source intelligence (OSINT) for the defense enterprise[M]. Santa Monica: Rand Corporation, 2018.
[13] MARTIN L. Gaining the advantage, applying cyber kill chain methodology to network defense [EB/OL]. [2023-06-01]. https://www. lockheedmartin. com/content/dam/lockheed-martin/rms/documents/cyber.
[14] STROM B E, APPLEBAUM A, MILLER D P. et al. MITREATT&CK: design and philosophy [EB/OL]. [2022-09-20]. https://www. mitre. org/sites/ default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy. pdf.
[15] OASIS. STIX version 2. 1 committee specification 02[EB/OL]. [2023-06-01]. https://oasis-open. github. io/cti-documentation/resources#stix-21-specification.
[16] BROWN P, ESTEFAN J A, LASKEY K, et al. Version 1. 0. committee specification draft 03 / public review draft 02 [EB/OL]. [2023-06-01]. https://Reference Architecture Foundation for Service Oriented Architecture Version 1. 0 (oasis-open. org).
[17] DARLEY T, KIRILLOV I, PIAZZA R, et al. CybOX version 2. 1. 1. Part 01: Overview OASIS committee specification draft 01/public review draft [EB/OL]. [2016-06-20]. https://CybOX™ Version 2. 1. 1. Part 01: Overview (oasis-open. org).
[18] THRON R, DIRNBERGER H, TJOA S, et al. Requirements and challenges for digital forensic readiness in industrial automation and control systems [C]//Proceedings of the 3rd International Conference on Industrial Engineering and Managemen. Barcelona, Spain:ACM, 2022:232-238.
[19] RAMADHAN R A, SETIAWAN P R, HARIYADI D. Digital forensic investigation for non-volatile memory architecture by hybrid evaluation based on ISO/IEC 27037: 2012 and NIST SP800-86 framework[J]. IT Journal Research and Development, 2022, 6(2): 162-168.
[20] ISO/IEC. 27043: 2015 Information technology - Security techniques- Incident investigation principles and processes [S]. USA:ICS,2015.
[21] GIBSON S D. Exploring the role and value of open source intelligence [M]//HOBBS C, MORAN M, SALISBURY D. Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities. London: Palgrave Macmillan, 2014: 9-23.
[22] ACLKALIN A. Integration of safety management effectiveness into QRA calculations[EB/OL]. [2009-04-16]. https://doi. org/10. 1002/prs. 10323.
[23] ENISA Threat Landscape. Bitdefender:Mid-year threat landscape report2020[J]. Computer Fraud & Security,2020(9):4.
[24] IZAR T, MATTHEW J C. Threat modeling: A practical guide for development teams[M]. California:O'Reilly Media,2020.
[25] DALZIEL H. Common objectives of a threat intelligence program [M]// How to define and build an effective cyber threat intelligence capability. USA:Elsevier Inc., 2021:13-14.
[26] CHISMON D, RUKS M. Threat intelligence: Collecting, analysing, evaluating[J]. MWR InfoSecurity Ltd., 2015, 3(2): 36-42.
[27] COFFMAN T, GREENBLATT S, MARCUS S, et al. Graph-based technologies for intelligence analysis [J]. Communications of the ACM,2004,47(3):45-47.
[28] ENESCU E, POSASCIU C, et al. Ethical issues in open source intelligence activity [J]. Romanian Intelligence Studies Review, 2010(4):14.
[29] CASANOVAS P. Open source intelligence, open social intelligence and privacy by design [C]//ECSI. Spain: CEUR Workshop Proceedings,2014: 174-185.
[30] GHIONI R, TADDEO M, FLORIDI L. Open source intelligence and AI: A systematic review of the GELSI literature[J]. AI & Society, 2024,39:1827-1842.
[31] FORCE N J T. NIST Special Publication 800-53 Revision 5-Security and Privacy Controls for Information Systems and Organizations [S]. Gaithersburg, USA: National Institute of Standards and Technology, 2020.
[32] DANDURAND L, SERRANO O S. Towards improved cyber security information sharing [C]//Proceedings of the 5th International Conference on Cyber Conflict (CYCON 2013). Piscataway NJ:IEEE, 2013: 1-16.
[33] JOHNSON C, BADGER L, Waltermire D, et al. NIST special publication 800-150: Guide to cyber threat information sharing [S]. Gaithersburg, USA: National Institute of Standards and Technology, 2016.
[34] 李留英. 美国网络威胁情报共享实践研究[J]. 信息安全研究, 2020,6(10):941-946.
[35] 朱琳. 网络安全信息共享制度研究[D]. 北京:北京邮电大学, 2018.
[36] 周秋君. 欧盟网络安全战略解析[J]. 欧洲研究,2015,33(3): 60-78,6-7.
[37] 李留英. 欧盟网络威胁情报共享进展及启示研究[J]. 情报杂志,2021,40(5):8-15.
[38] SIMOLA J. Enhancing the European cyber threat prevention mechanism[J]. Journal of Information Warfare, 2021, 20(1): 17-32.
[39] BARNUM S. Standardizing cyber threat intelligence information with the structured threat information expression (stix) [J]. MITRE Corporation, 2012, 11: 1-22.
[40] DEMCHENKO Y. The incident object description exchange format[J]. RFC,2007,5070:1-92.
[41] UNGUREANU G T. Open-source intelligence (OSINT). The way ahead [J]. Journal of Defense Resources Management (JoDRM), 2021, 12(1): 177-200.
[42] CAICT. 大数据白皮书(2016 年)[R]. 北京:中国信息通信研究院(工业和信息化部电信研究院),2016.
[43] FRANKLIN M. The berkeley data analytics stack: Present and future[C]//Proceedings of the IEEE International Conference on Big Data. Piscataway, NJ: IEEE, 2013: 2-3.
[44] 赵颖,王权,黄叶子,等. 多视图合作的网络流量时序数据可视分析[J]. 软件学报,2016,27(5):1188-1198.
[45] 程学旗,靳小龙,王元卓,等. 大数据系统和分析技术综述[J]. 软件学报,2014,25(9):1889-1908.
[46] NAINGGOLAN D R M. Data science, big data, and predictive analytics: A platform for cyberspace security intelligence [J]. Jurnal Pertahanan & Bela Negara, 2017, 7(2): 19-36.
[47] 陈兴蜀,曾雪梅,王文贤,等. 基于大数据的网络安全与情报分析[J]. 工程科学与技术,2017,49(3):1-12.
[48] 张繁,谢凡,江颉. 网络威胁安全数据可视化综述[J]. 网络与信息安全学报,2018,4(2):34-39.
[49] 王智民,武中力. 未知威胁的定义与检测方法综述[J]. 工业信息安全,2022(4):39-47.
[50] 王一丰,郭渊博. 数据驱动的未知网络威胁检测综述[J]. 信息安全与通信保密,2022(10):86-97.
[51] HEY A J, TANSLEY S, TOLLE K M, et al. The fourth

paradigm: Data-intensive scientific discovery[M]. Redmond, USA: Microsoft Research, 2009.
[52] ADEWOPO V A. Exploring open source intelligence for cyberthreat prediction[D]. Nigeria: Lead-City University, 2019.
[53] CHOO K K R. Research Challenges and Opportunities in Big Forensic Data [C]// Proceedings of the 2017 International Workshop on Managing Insider Security Threats (MIST′17). Dallax, USA: ACM, 2017: 79-80.
[54] SEBASTIAN K, MANDY K, TIM H S. Machine learning and cyber security [J]. Information Technology, 2023(5): 142-154.
[55] ARP D, QUIRING E, PENDLEBURY F, et al. Dos and don′ts of machine learning in computer security [J]. arXiv preprint arXiv, 2010.09470, 2021.
[56] DIONÍSIO N, ALVES F, FERREIRA P M, et al. Towards end-to-end cyberthreat detection from Twitter using multi-task learning [C]//2020 International Joint Conference on Neural Networks (IJCNN). Piscataway, NJ: IEEE, 2020: 1-8.
[57] 孙天放. 基于深度学习的威胁情报信息抽取研究[J]. 现代计算机, 2021(16): 59-64.
[58] 王淮, 杨天长. 网络威胁情报关联分析技术[J]. 信息技术, 2021(2): 26-32.
[59] 罗琴, 杨根, 刘智, 等. 结合主动学习的威胁情报 IOC 识别方法[J]. 电子科技大学学报, 2023, 52(1): 108-115.
[60] 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.
[61] 陈剑锋. 网络空间开源威胁情报分析的人机优化策略研究[J]. 信息安全与通信保密, 2022(7): 17-24.
[62] SURYOTRISONGKO H, MUSASHI Y, TSUNEDA A, et al. Robust botnet DGA detection: Blending XAI and OSINT for cyber threat intelligence sharing[J]. IEEE Access, 2022, 10: 34613-34624.
[63] PERRINA F, MARCHIORI F, CONTI M, et al. AGIR: Automating Cyber Threat Intelligence Reporting with Natural Language Generation[J]. arXiv preprint arXiv, 2310.02655, 2023.
[64] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
[65] 黄克振, 连一峰, 冯登国, 等. 基于区块链的网络安全威胁情报共享模型[J]. 计算机研究与发展, 2020, 57(4): 836-846.
[66] 冯景瑜, 张琪, 黄文华, 等. 基于跨链交互的网络安全威胁情报共享方案[J]. 信息网络安全, 2022, 22(5): 21-29.
[67] 姜鑫, 王飞. 基于联盟区块链的网络威胁情报共享平台[J]. 电脑与信息技术, 2022, 30(1): 50-52.
[68] 史慧洋, 刘鹏, 王鹤. 基于区块链和神经网络的威胁情报评估[J]. 天津大学学报(自然科学与工程技术版), 2022, 55(5): 527-534.
[69] 程叶霞, 付俊, 陈东, 等. 基于区块链的威胁情报共享及评级技术研究[J]. 信息通信技术与政策, 2020(2): 19-24.
[70] PREUVENEERS D, JOOSEN W, BERNAL B J, et al. Distributed security framework for reliable threat intelligence sharing[J]. Security and Communication Networks, 2020, 2020: 8833765.
[71] PREUVENEERS D, JOOSEN W. Sharing machine learning models as indicators of compromise for cyber threat intelligence [J]. Journal of Cybersecurity and Privacy, 2021, 1(1): 140-163.
[72] BAR-ILAN J. Data collection methods on the Web for infometric purposes—A review and analysis[J]. Scientometrics, 2001, 50: 7-32.