电信运营商威胁情报体系研究与应用探索

张海涛，蒋熠，竺士杰，陈琦
（中国移动通信集团浙江有限公司，浙江 杭州 310051）

摘　要：随着互联网时代网络攻防的不对等加剧，威胁情报成为缩小这种差距的重要工具之一。在研究分析了威胁情报国内外研究现状的基础上，提出了一套适用于电信运营商的威胁情报体系构建方法，包括制定计划、情报生产、情报分析、情报管理、情报共享和情报应用 6 个环节。基于该体系架构提出了一套多源情报融合评估机制，概述了情报聚合分析、情报信誉分析、情报关联分析和情报老化分析 4 个阶段涉及的技术和建设方法，帮助电信运营商构建情报融合分析能力。同时，针对入侵类和失陷类情报领域给出了情报生产和同步应用原则，为电信运营商应用威胁情报技术构建安全防护体系提供了有益的参考。

关键词：威胁情报；情报分析；情报生产；情报应用；电信运营商
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000–0801.2022293

Research and application exploration of threat intelligence system of telecom operators

ZHANG Haitao, JIANG Yi, ZHU Shijie, CHEN Qi
China Mobile Communications Zhejiang Co., Ltd., Hangzhou 310051, China

Abstract: With the increasing inequality of network attack and defense in the Internet era, threat intelligence has become one of the important tools to narrow this gap. Based on the analysis of the research status of threat intelligence at home and abroad, a set of construction methods of threat intelligence systems suitable for telecom operators were proposed, including six steps: intelligence planning, intelligence production, intelligence analysis, intelligence management, intelligence sharing and intelligence application. Meanwhile a set of multi-source intelligence fusion assessment mechanisms was presented, and the technologies and methods were systematically expounded involved in the four stages of intelligence aggregation analysis, intelligence reputation analysis, intelligence correlation analysis and intelligence aging analysis, so as to help the telecom operators build the ability of intelligence fusion analysis. At the same time, the principles of intelligence production and synchronous application were given for intrusion and loss intelligence, which provided a useful reference for telecom operators to apply threat intelligence technology to build a security protection system.

Key words: threat intelligence, intelligence analysis, intelligence production, intelligence application, telecom operator

收稿日期：2022–06–21；修回日期：2022–12–06

0 引言

随着信息技术的发展和移动通信技术的普及，传统的网络安全防御边界正在逐渐消失。国家互联网应急中心[1]的研究显示：我国已逐渐成为各类网络攻击的重灾区，其中以高级持续威胁（advanced persistent threat，APT）和分布式拒绝服务（distributed denial of service，DDoS）攻击为代表的新型攻击尤其明显[2]。随着网络攻防不对等趋势的加剧，传统基于防火墙、入侵检测系统（intrusion detection system，IDS）、防毒墙的孤岛式防御方式已无法应对日益复杂多样的攻击方式。威胁情报能力已成为安全行业解决“攻防信息不对等”，构建“联防联控”动态立体防御局面不可缺失的基础能力之一，并得到行业广泛认可。目前针对威胁情报的定义存在多种方式，根据 Gartner 在“Market Guide for Security Threat Intelligence Products and Services”中的定义，威胁情报可被理解为“威胁情报是一种基于证据的知识，包括了情境、机制、指标、隐含和实际可行的建议”[3]。

1 威胁情报国内外研究现状

随着安全行业对威胁情报的关注，威胁情报逐步从概念到落地，大量公司在威胁情报领域投入大量的精力。第一类是传统大型安全厂商，如绿盟科技、启明星辰；第二类是新兴的安全创业公司，如微步在线、天际友盟，还有传统杀毒厂商，如 360、Symantec 和 FireEye；第三类是网络硬件厂商，如思科和华为；最后则是运营商专业子公司，运营商具备海量基础数据的资源优势，近年来也开始自发研究威胁情报，如移动研究院、电信云堤。国内外针对威胁情报的研究可谓“百家争鸣，万花齐放”。

1.1 国外研究现状

2001 年的“9·11 恐怖袭击事件”让美国政府认识到前沿信息技术分析能力的重要性。美国政府在 2010 年发布了《国土安全网络和物理基础设施保护法》，2013 年发布了第 13636 号行政命令《提升关键基础设施的网络安全》（EO-13636）[4]提出 2013 年发布了第 21 号总统令《关键基础设施的安全性和恢复力》（PDD-21）[5]，2015 年发布了《网络安全信息共享法案》[6]，这些法令不断提出信息共享和威胁情报要求。美国政府为了让政府、企业能够建立系统科学的威胁情报能力，于 2016 年发布了“NIST SP800-150: Guide to Cyber Threat Information Sharing”[7]，用于指导美国各界组织建立威胁情报能力。一些部门行业组织，如 MITRE 等，发布了一些威胁情报建议性行业标准，如 STIX、TAXII 等，对威胁情报的存储和共享等方面给出业界通用建议[8-13]。此后，基于国家政策和标准，美国的威胁情报工作取得了实质性的进展，为美国的信息安全提供了全球领先的安全防护能力。

1.2 国内研究现状

在威胁情报领域，国内起步相比欧美国家较晚，但是我国对威胁情报比较重视。2017 年《网络安全法》第二十九条对信息收集、合作与建立相关行业标准和协作机制提出了积极的指导意见。2018 年国家标准《信息安全技术 网络安全威胁信息格式规范》（GB/T 36643—2018）[14]提出提高国内威胁情报建设及共享的规范性，推动国内威胁情报共享生态形成。2020 年公安部发布《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》[15]，指出“全面加强网络安全防范管理、监测预警、应急处置、侦查打击、情报信息等各项工作”。

除了政策推进，基础电信运营商作为庞大基础通信网络服务的提供商，利用威胁情报预防各种威胁是其职责之一。近年来电信运营商在威胁情报方面的建设较为不足，威胁情报运营体系不够完整，对于庞大的监测设备告警数量、国家级安全机构发布的威胁情报和安全厂商提供的威胁

情报，仅有安全人员自行了解，没有进行系统高效的运营应用。

综上所述，电信运营商有必要构建一套适用于自身业务发展的威胁情报体系和多源情报融合的评估机制，强化对威胁情报的应用，提升大数据分析与安全防护的实力。

2　威胁情报体系构建

结合互联网背景以及国内外现状，本文提出一套企业或组织从无到有构建威胁情报能力的体系方法，威胁情报体系如图 1 所示，整个流程包括制定计划、情报生产、情报分析、情报管理、情报共享和情报应用 6 个环节。按照时间顺序，每个环节环环相扣、缺一不可，通过 6 个环节构建了满足电信运营商自身需求且发挥应用价值的情报能力。

2.1　制定计划

制定计划包括 5 个环节，通过 5 个环节的周密部署保证后续能力建设的顺利开展，并达到预期目标。

（1）明确情报需求：建设威胁情报前，需要分析自身的情报需求，而不是盲目地建立威胁情报体系。情报需求要根据自身应用场景确定，例如，攻击检测与防御场景需要将情报集成到现有防御设备中，实现和安全产品联动工作；威胁狩猎场景需要积累一定量的失陷检测（indicator of compromise，IOC）情报，帮助安全人员更全面地分析等。

（2）梳理外部情报源：建立威胁情报能力，特别是在前期，难免需要借助外部能力，因此建设前需要先明确自身有哪些情报源、这些情报源是否有自身想要的情报以及与外部情报数据的对接问题。

（3）梳理内部情报源：引入外部情报源的同时，需要梳理自身内部是否具备情报生产能力，有哪些情报生产渠道或数据。

（4）制定情报计划：梳理好全部情报源之后，制定情报从生产到应用的技术架构，包括威胁情报数据的采集接入和存储管理、关联挖掘分析、共享输出、应用服务以及情报管理。

（5）情报生产实施：正式建设开始能力前，需要评估团体内部能够给予的政策或资源的支撑力度，这是后续工作能够开展的前提。

2.2　情报生产

威胁情报生产能力是威胁情报能力构建的基础，没有情报生产能力，威胁情报就会变成无源之水。

（1）开源情报：很多情报厂商或安全厂商（国外）会将威胁情报数据开源到互联网上，因此开源情报是一个比较好的情报获取渠道，该类数据的广度和深度也会在一定程度上影响数据的关联分析深度，因此需要保证数据的持续性、准确度和新鲜度。而且在接入开源情报时，需要谨慎评估情报可靠性，避免数据污染。开源情报清单见表 1。

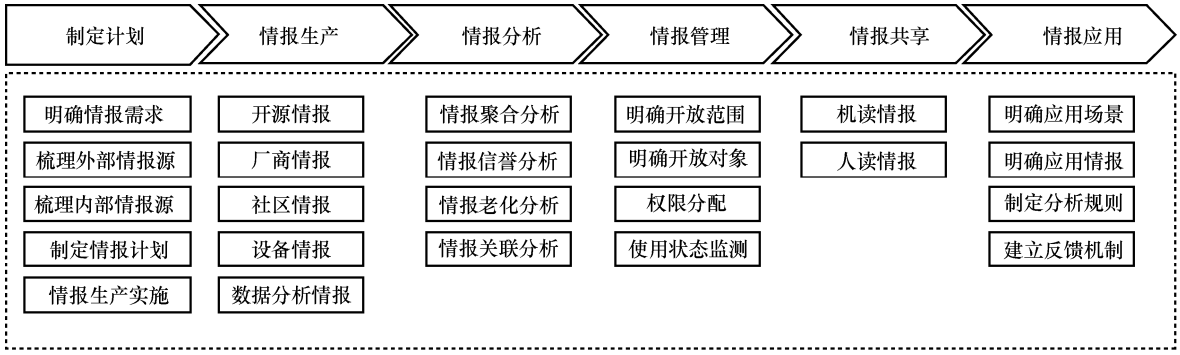

图 1　威胁情报体系

表 1　开源情报清单

公司	说明
PhishTank	该开源网站对外输出钓鱼网站情报信息
Zeustracker	该开源网站对外输出恶意软件情报信息
Feodo Tracker	该开源网站对外输出僵尸网络控制端情报信息
OpenPhish	该开源网站对外输出钓鱼网站情报信息
Ransomware Tracker	该开源网站对外输出恶意软件情报信息
Cybercrime Tracker	该开源网站对外输出恶意软件情报信息
UCEProtect	该开源网站对外输出邮件黑名单情报信息

（2）厂商情报：为了获取比较高质量的可靠情报，可以考虑通过商业厂商获取，2021 年 Gartner 发布了“Market Guide for Security Intelligence Products and Services”，其中推荐了部分比较成熟的情报厂商。部分比较成熟的情报厂商见表 2。

（3）社区情报：社区情报的初衷就是打破传统依托安全服务商提供情报的局面，将客户或用户纳入自己的情报生产机制，构建“人人都是情报生产者”的良性生态。

（4）设备情报：很多公司部署了大量的安全设备，安全设备产生的可信告警本身就是很好的获取威胁情报的途径。网络基础设施自身的安全检测防护系统除了可以直接消费已有的外部情报数据，加强自身的御能力，还能把自身检测到的威胁告警信息反馈给网络基础设施，进一步增强网络空间防御能力，是基础电信运营商威胁情报的一个重要来源。

（5）数据分析情报：很多公司（如运营商）掌握着大量的网络数据，这些数据通过大数据或 AI 技术分析后可以挖掘情报。

2.3　情报分析

对于通过开源、商业等渠道获取的多源情报数据，需要先采用大数据分类技术，对海量数据进行分类整理，然后进行情报分析，使之成为规范化的、可用的情报。情报分析过程主要包括情报聚合分析、情报信誉分析、情报老化分析和情报关联分析几个环节。

（1）情报聚合分析：情报的数据来源非常广泛，对原始数据进行预处理，规范数据格式，对数据的合法性和准确性进行消重、校验，去掉脏数据，实现多源数据清洗，确保数据的有效性。主要通过 IP 行为画像、身份属性多层关联、推理路径求证、信誉衰减老化机制、采集路径溯源机制等进行情报清洗。首先将不同数据源的信心指数划分为不同等级，并设置老化机制，保证情报数据的质量。同时分析引擎可提炼 IP 的 profile 属

表 2　部分比较成熟的情报厂商

公司	说明
微步在线	微步在线被称为中国新一代网络安全公司代表、威胁情报领军企业，提供专业的安全即服务（security-as-a-service，SecaaS）
奇安信	奇安信是中国网络安全公司之一，专门为政府、企业、教育、金融等机构和组织提供企业级网络安全技术、产品和服务
神州绿盟	神州绿盟是中国网络安全公司之一，主要提供安全类产品服务和解决方案，包括漏洞扫描、Web 应用防火墙（Web application firewall，WAF）、IDS 等安全检测和防护类产品
CrowdStrike	CrowdStrike 是全球知名的下一代终端安全厂商，成立于 2011 年，于 2012–2013 年推出拳头产品威胁情报服务 Falcon X 及终端检测与响应（endpoint detection and response，EDR）产品 Falcon Inshight
Cyberint	Cyberint 是一家以色列的安全公司，提供数字风险保护和威胁情报解决方案保护服务，并在数据或资产暴露时发出警报
Cyware Labs	Cyware Labs 是一家美国网络融合解决方案提供商、一家提供威胁情报共享和网络融合产品的网络安全公司，为组织建立虚拟网络融合中心所需的技术提供了支持
ThreatConnect	ThreatConnect 成立于 2011 年，是一家威胁情报公司，主打产品是威胁情报平台，这套平台提供 3 个主要功能：整合情报、分析情报和支撑行动

性及恶意行为属性，并通过部署在互联网的 NetFlow 特征判断 IP 是否存在可疑的恶意行为，如是否为扫描 IP 或垃圾邮件 IP 等，并对具有相同异常行为的 IP 等进行聚类分析，提升恶意行为判断的准确性。另外，还可通过多层关联，一旦发现某 IP、某域名等关联了已被判断为恶意的样本、域名、样本、URL 等，其威胁信誉等级的恶意度评级也会提高，并会在其安全评分中加入该关联判断权重。

（2）情报信誉分析：结合各个信誉源的子层评估要素和资产关联性，综合输出威胁度（threat）、脆弱性（vulnerability）和可信度（confidence）3 个顶层数字化指标，满足人读的感知性需求和机读的自动化需求，助力安全评估和态势感知的自动化。

（3）情报老化分析：基于当前时间、攻击时间、威胁类型等进行差异化、细粒度情报老化分析，避免误报，造成业务误拦截。

（4）情报关联分析：关联分析的重点在于能从多种维度的情报数据集合中，发现待查数据的关联关系。不同对象之间完成数据标准化后，需要对海量不同来源和不同维度的数据、事件进行关联分析，对情报进行二次验证分析，从而筛选出准确率高、可追溯的高级威胁攻击信息。通过长时间的关联，安全分析人员可挖掘某台主机、某个用户的异常行为，从而实现不基于签名的未知攻击检测。对于每一条可疑报警，分析人员可以查询与该报警相关的各类数据，从而确定报警真实性、攻击源，评估攻击造成的危害，实现对多源异构的数据进行高效检索和对海量的关联关系进行聚类挖掘。大数据关联分析应对的是海量安全数据的关联分析，该引擎首先从外部输入数据（包括但不限于威胁情报、告警日志、NetFlow 和域名系统（domain name system，DNS）记录）中提取出五大关联关系，包括网络行为关联关系、指向关系、从属关系、时频关联性和相似性关联性，并将其作为引擎的分析输入。在关联分析中，该引擎能够进行维度的拓展、级联的关系搜索和关联关系的特征泛化，同时可根据自定义规则进行清洗和提纯，最后应用评价算法综合评估关联分析结果，进行威胁重新定性。

2.4　情报管理

存储的情报类型包括基础情报、高级威胁情报和定制情报等。其中，基础情报包括 IP 指纹、Web 指纹、IP 信息、域名信息、漏洞库、样本哈希、IP IOC、域名 IOC、URL IOC、文件 IOC、数字证书等；高级威胁情报包括事件情报、攻击组织情报、攻击工具情报、高级威胁分析报告、安全事件分析报告等；定制情报包括周期性威胁播报、热点威胁分析报告、行业威胁分析报告、资产威胁分析报告等。

针对不同类型威胁情报需要做好 4 个方面的管理，包括明确开放范围、明确开放对象、权限分配和使用状态监测。

（1）明确开放范围：在情报数据中部分内容可能会涉及敏感数据，因此在开放过程中需要明确自身情报内容可以开放的范围，避免敏感信息泄露。

（2）明确开放对象：在情报开放过程中需要对开放的对象进行评估，不同的对象需要的情报内容及情报同步方式均不相同，需要充分考虑开放对象的需求。

（3）权限分配：在情报开放过程中，针对不同的用户需要设置不同的权限，包括但不限于查看内容权限、操作权限等。

（4）使用状态监测：在威胁情报能力对外输出过程中需要具备对用户使用状态的监测能力，一方面保证服务可用，另一方面也可以处理一些恶意爬虫等非法行为。

2.5　情报共享

情报共享需要考虑机读情报和人读情报需求，因此建议至少具备应用程序接口（application

programming interface，API）和 Web 两种情报查询方式，满足不同的消费对象及场景需求。

（1）机读情报：提供 API 情报共享方式，满足设备或系统大并发、低时延调用需求。

（2）人读情报：提供 Web 查询、邮件发送等人读情报共享方式，满足人读情报查询方便、数据结构清晰且易于理解的需求。

2.6 情报应用

在威胁情报建设领域，科学的情报应用机制往往被忽略，但是这个环节却是情报能否发挥其价值的关键。该环节主要包括明确应用场景、明确应用情报、制定分析规则和建立反馈机制 4 个关键环节。

（1）明确应用场景：明确应用场景是后续明确应用情报和制定分析规则的前提，不同的应用场景存在巨大的区别，例如，入侵类和失陷类场景、实时类和离线类场景在情报应用领域存在很大的差别，如果不能定义好，应用好情报就无从谈起。

（2）明确应用情报：不同的应用场景需要应用不同的情报，只有“对症下药”才能够“事半功倍”，否则会“劳而无功”。例如，失陷类场景需要计算机与通信（computer & communication，C&C）或恶意软件下载类情报，入侵类场景更多的是需要漏洞攻击和 Web 攻击等类型的情报。

（3）制定分析规则：不同应用场景需要不同类型的情报，制定不同的分析方法，以达到自身的预期。例如，对会话日志分析需要使用 IP 情报，同时也要结合端口、频次等内容进行综合分析才可以达到预期效果，一个远控 IP 也有可能作为一个扫描类地址对外使用，如果仅仅根据访问 IP 为远控 IP 就定义为失陷（即认为机器已被木马控制）就是错误的。

（4）建立反馈机制：大部分安全运营工作缺少反馈环节，导致大部分安全告警仅存在于告警环节，未建立闭环验证机制。因此在威胁情报应用中必须建立反馈机制，从而验证情报使用是否正确，进而提高情报质量和改进使用方法。

3 多源情报融合评估机制

多源情报融合包括情报采集、加工和分析融合等过程，情报采集源包括安全厂商情报、开源厂商情报、安全监测情报和安全事件情报，各类情报经过预处理后进行分析融合，最终形成情报库，甚至情报作战地图。多源情报融合评估机制如图 2 所示。

3.1 情报聚合分析机制

不同来源情报的源字段种类、字段类型、字段定义方式、字段描述方式等均不相同，甚至不同来源的情报还会存在冲突矛盾情况，因此需要对多源情报进行数据归一化、数据去噪和数据融合等处理，使情报达到一种稳定规范的形态。例如，一次 Web 攻击可能包含上万次攻击子事件，就需要将其融合为一个攻击事件。在情报中也会存在字段命名不一致甚至缺失的情况，这也需要进行统一的命名，补齐缺失的字段或者删除冗余的字段。

（1）情报数据标准化：为每一类情报定义标准格式规范，以统一存储格式，进行高级别的威胁情报分析和使用。标准规范的制定既参考国内外已有标准规范又遵照业界事实标准，同时满足威胁情报的各种使用场景需求，兼顾内部使用和跨企业的情报交换。

（2）情报数据归一化、去噪和融合：利用多种验证手段去除不准确数据，这是保证情报质量的关键。目前主要综合采用聚合画像矩阵、关联验证、证据验证等技术进行情报质量检测和甄别。

例如，IP 聚合画像矩阵拥有四大类数 10 种标签，其中包含归属类属性集、服务类属性集、告警类属性集和行为类属性集。丰富的数据剖面设计为后续的多维度评估提供了大量的选择空间，增强了评估的可信度和全面性；同时给前端用户

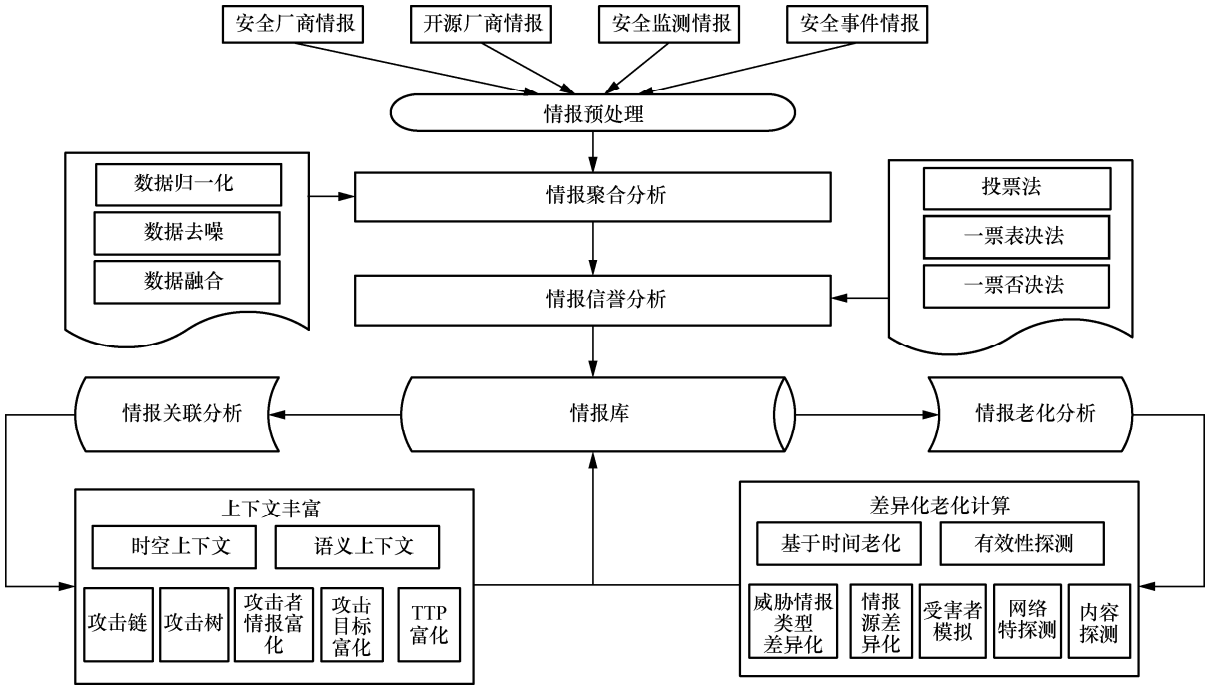

图 2　多源情报融合评估机制

和后端数据分析员迭代式分析和交叉验证提供了依据，提升了人工交互的可操作性和便捷性。

关联验证主要根据情报内容进行多类情报的递归关联，通过检测多情报间的一致性发现情报冲突，联合情报上下文和置信度剔除低质量情报。

证据验证通过对情报数据的支持证据链的可靠性核查判断情报数据的可靠性，剔除没有可靠证据支持的情报数据。

3.2　情报信誉分析机制

不同来源情报的威胁等级及置信度等均存在区别，特别是开源网站情报的误报现象更加严重，因此需要有一套科学的机制判定情报是否可信，并给出科学的威胁定级。常见的情报信誉分析方式包括投票法、一票表决法、一票否决法等。投票法可以理解为常见的选举投票，当多个情报源存在属性定义冲突时，可以通过少数服从多数的机制给出最终的决断。一票表决法是指对某一情报源采取绝对信任的机制，对某一情报源属性定义（是否恶意）无条件信任，其他结果依从该结果。一票否决法最常见的就是白名单机制，对于白名单中的内容，即使某一情报源认为其是恶意的，也不判定其是恶意的。威胁情报信誉分析实践中的优先级由高到低分别为：一票否决法、一票表决法、投票法。在社会行为中投票法往往占主导地位，但是在威胁情报实践中则恰恰相反，这是因为大部分开源情报会有大量不可信的情报，而开源情报会被部分情报厂商收录，最终可信度最低的开源情报有可能会被误判为最可信的情报，从而导致误判。

整个情报信誉分析过程会筛选出关键情报供专家进行分析和评估，进而发现更深层次的情报。

3.3　情报关联分析机制

在威胁情报领域，大部分情报是孤立的，会导致其价值在一定程度上被衰减，因此需要通过情报关联分析机制，由点到面，最终形成一个情报网或情报地图，从而指导人们制定安全领域的作战方向甚至战略方向。最基本的情报线条梳理包括攻击者（攻击者，包括组织、团伙、家族等）是谁、在什么时间（攻击时间）、为了什么目的（攻

击企图，包括窃密、勒索、挖矿等）、对谁（攻击对象，包括学校、科研院所、政府单位等）发起了攻击。同时，数据本身还存在交叉信息，以域名为例，包括 whois 信息、互联网内容提供者（Internet content provider，ICP）备案信息、passive DNS 信息、域名关联文件信息、域名关联事件信息、域名关联证书信息、域名端口服务信息、域名对应网站使用组件信息等。

在此机制中，应对的是海量安全数据的关联分析。其输入数据包括但不限于以下几种。

（1）威胁情报：包括 IP 定性、域名定性、IP 分类数据。

（2）告警日志：安全设备数据。

（3）NetFlow：包括恶意源 IP 发现（DDoS、病毒邮件源）、历史 Flow 库数据。

（4）DNS：包括恶意域名发现、域名识别、查询频率异常、flux 检测、多层 C&C 发现）、历史解析审查数据。

将外部数据输入引擎后首先进行关联关系的分析，提取出五大关联关系，包括网络行为关联关系、指向关系、从属关系、时频关联性和相似性关联性，然后将提取出的关联关系输入分析引擎。分析引擎中主要包含以下子引擎。

（1）维度关联拓展引擎：主要针对定性数据、行为数据、告警数据进行维度关联分析。

（2）级联关系搜索引擎：主要进行图计算、快速索引、递归查找等分析。

（3）特征泛化引擎：主要进行流量特征、行为特征、特征泛化、时频特性、互联度等的泛化分析。

（4）大数据清洗提纯引擎：可以区分出非扫描数据、非 CDN 数据等数据。

（5）自动化评价引擎：可以自动给出 C&C 评分、周期性评分等评价。

通过以上分析处理，分析引擎可以给出关联分析结果，包括关联线索、关联资产、关联事件，同时还可以给出对关联分析结果的评估。

3.4 情报老化分析机制

情报与传统的军事情报和新闻消息等有一个共同的特点，那就是时效性，时效性决定了情报的价值。情报的时效性主要包括两个维度，分别为获取情报的及时性和情报的有效时间。获取情报的及时性决定了安全防护和运营的价值，获取情报的时间越早越可以缩短攻防不对等的时间，使威胁情报“多点感知，全网联动”防御的价值更加显性化。情报的有效时间有利于人们在安全实践中关注最重要的情报，做出最正确的决策，避免情报误判、拦截正常用户、影响正常业务。要保证情报时效性就必须建立一套科学的情报老化机制。在情报老化分析中绝不是“一刀切”的情报老化。基于不同的情报源、不同的威胁类型存在不同的老化机制。例如，失陷类情报具有比入侵类情报更长的存活时间，在失陷类情报中，远控类情报的存活时间比钓鱼类情报长，在远控类情报中，普通远控类情报的存活时间比 APT 类远控情报长（APT 反侦察能力较强，攻击资源丰富，更换远控地址比较敏捷快速）。基于时间的老化其实仅是一种折中的选择，例如，若一个域名通过其他手段可以验证其为有一个有效的钓鱼域名，那么不管过去时间长短，均认为该域名为存活域名。

4 情报分类及应用探索

从电信运营商的整体应用维度出发，威胁情报可以分为两个维度，分别为入侵类情报和失陷类情报。入侵类情报和失陷类情报的生产及联动防御流程如图 3 所示。

4.1 入侵类情报生产及联动防御

在入侵类防护场景中，如 WAF、防火墙、业务风控等，需要对入侵类 IP 进行告警或拦截。但是入侵类情报具有时效性短且存在多用户公用问题，因此对入侵类 IP 进行拦截成为一个难题。

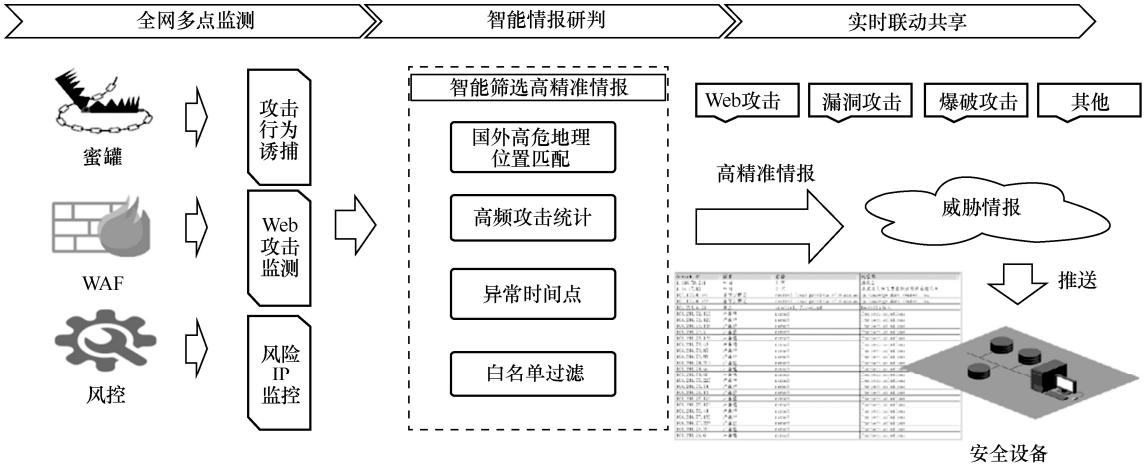

图 3　入侵类情报和失陷类情报的生产及联动防御流程

时间窗口控制机制：与失陷类情报相比，入侵类情报具有更加小的时间窗口，因此它的及时性非常重要，理想状态为 A 地区发现攻击后，B 地区能够在 1 s 内收到入侵情报，提前进行封堵，避免受到影响，且封堵时间不会过长，避免影响正常用户。

用户属性控制机制：入侵防护类系统都有被防护的业务系统，业务系统都有其对应的用户群体。基于用户群体可以区分哪些入侵类攻击 IP 可以直接拦截，哪些不可以拦截。例如，一个网站面向的用户为国内用户，对于近期发起过入侵攻击的国外 IP，基本可以直接拦截封堵；进一步地，同样是国内用户 IP，如果访问 IP 为互联网数据中心（Internet data center，IDC）属性 IP 则可以直接封堵，如果是家庭带宽或 5G 网络的 IP 就不可以直接封堵，因为即使该 IP 近期发起过攻击行为，但是该 IP 由很多家庭用户共用，直接封堵会导致正常用户的访问也被封堵，可能会收到用户投诉，出现生产事故。

异常时间点控制机制：针对用户访问群体的正常访问时间段进行控制，对于异常时间段内曾经近期发起过攻击的 IP，可以选择性地采取拦截措施。例如，大部分用户访问发生在白天，若发现凌晨 2 点有近期发起过攻击的 IP 访问，则可以采取一定程度的风控措施。

访问频率控制机制：针对用户群体的正常访问频率，结合自身业务进行画像，如果发现某 IP 的访问频率异常升高，则很大可能存在问题，同时如果该 IP 刚刚对其他系统发起过攻击，则可以直接封堵。

4.2　失陷类情报生产及联动防御

由于入侵类情报存在多用户属性，因此对其管控相对谨慎，并且由于大部分入侵类情报仅存在攻击行为，未必可以成功入侵系统，因此风险等级比失陷类情报低。失陷类情报供服务端使用，因此其情报有效时间更长，危害也更大。如果发现内部资产与失陷类情报（特别是远控类情报）通信，则基本可以断定该资产已经被黑客组织控制，属于比较重大的安全事件。

目前危害较大的 4 种失陷类情报包括：远控类情报、恶意软件类情报、挖矿类情报和钓鱼类情报。

远控类情报：远控类情报大部分为病毒或木马的反向代理控制后门地址，黑客通过该地址对受害者机器下发控制指令、窃取机密数据等。

恶意软件类情报：黑客通过更改地址实现受害者木马持久化，但是其危害比远控类情报弱，下载恶意软件并不代表该木马可以在潜在受害者机器上运行，未必会真正地感染失陷。

挖矿类情报：挖矿地址是挖矿木马反向连接

的地址，若存在通信行为，则该潜在受害者可能已被植入挖矿木马，危害较大。

钓鱼类情报：钓鱼网站是指欺骗用户的虚假网站。钓鱼网站的页面与真实网站的页面基本一致，欺骗消费者或者窃取访问者提交的账号和密码信息。

4.3 基于威胁情报和电信运营商网络的 APT 治理

以 APT 为代表的网络空间攻击成为各国博弈的新战场，电信运营商承载着国家关键基础设施的运营商网络，是 APT 攻击的潜在重点目标之一。电信运营商可以基于其运营商网络构建全方位、立体的监测体系。基于威胁情报和电信运营商网络的 APT 治理流程如图 4 所示。

数据布控：电信运营商布控的网络整体可以分为两大类，一类为 CMNet，另一类为 IP 承载网。IP 承载网主要供电信运营商内部使用，主要用于对自有设备遭受 APT 攻击的情况进行监测。CMNet 承载着电信运营商自己以及客户的网络流量。通过在 IDC 机房出口深度包检测（deep packet inspection，DPI）、网管网出口 DPI 和省网出口 DPI 布控，实现对发生在电信运营商网络上的 APT 攻击进行有效覆盖。

攻击线索分析关键技术：对于通过 DPI 采集上报的数据，通过威胁情报、沙箱、杀毒引擎、机器学习和通信特征检测规则等构建 APT 攻击线索发现还原能力。特别是通过沙箱、机器学习技术的引入，可以实现对未知威胁的检测。

归因溯源：首先通过威胁建模分析技术实现对攻击模式、攻击链条、受害者的分析。同时，利用线索拓线进一步进行组织归因和溯源反制。

4.4 基于威胁情报的自动化安全运营

入侵类、挖矿类情报通过安全态势感知中心进行格式标准化后，根据不同的应用场景设定不同危害等级并开展联动处置。处置方式可以基于人工分析告警增强方式，也可以基于安全编排自动化与响应（security orchestration, automation and response，SOAR）方式联动应急处置设备开展联动应急处置。

SOAR 将人、安全技术、流程和威胁情报进行深度融合；通过 playbook 剧本串/并联构建安全事件处置的工作流，自动化触发不同安全设备执行响应动作。在这个过程中，情报发挥了预警支撑和取证的重要作用。

依托威胁情报支撑，可以及时洞悉资产面

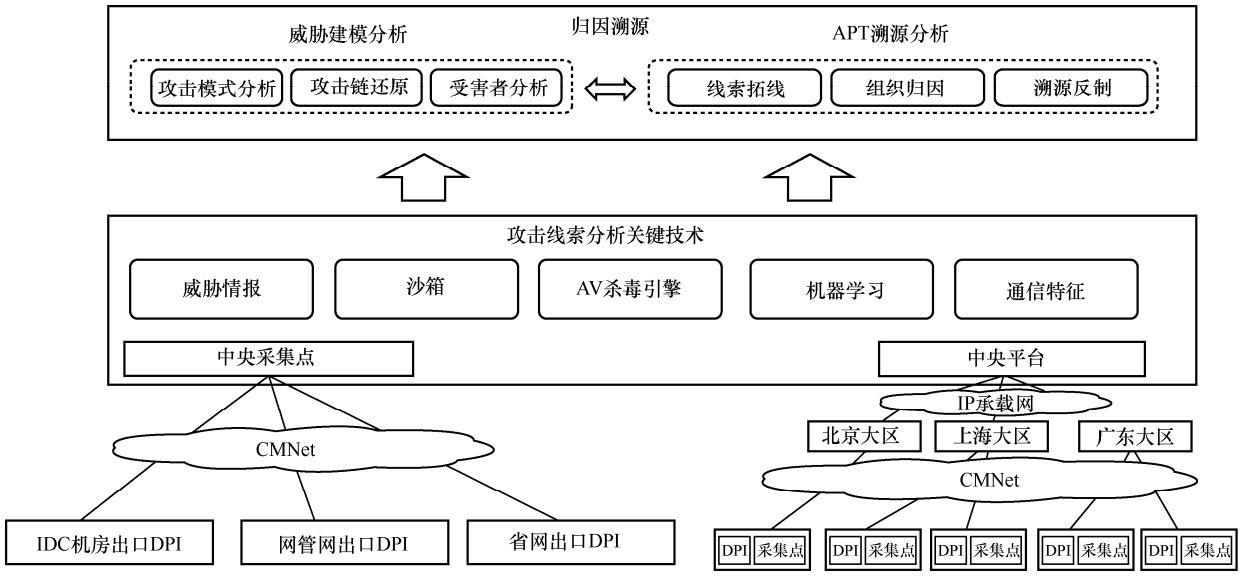

图 4 基于威胁情报和电信运营商网络的 APT 治理流程

临的安全威胁并进行准确预警，了解最新的挖矿、漏洞等威胁动态，实施积极主动的威胁防御和快速响应策略，结合安全数据的深度分析全面掌握安全威胁态势，并准确地进行威胁追踪和攻击溯源。

情报取证可选择情报类型（含 IP、统一资源定位符（uniform resource locator，URL）、样本、域名、C2、APT 等）、情报对象具体值（IP、URL、Domain、MD5）、执行结果（是否命中）进行匹配。

整个流程基于对安全事件上下文更加全面、端到端的理解，有助于将复杂的事件响应过程和任务转换为一致的、可重复的、可度量的和有效的工作流，变被动应急响应为自动化持续响应。基于威胁情报的自动化威胁处置响应如图 5 所示。

5　结束语

威胁情报在当前攻防不对等的局面中为网络安全建设和运营带来了曙光。通过威胁情报构建一套网络安全监测的天网，打破了传统孤岛式防御方式中存在的信息封闭、各自为战的局面，通过威胁情报的引入，实现了“多点感知，全网联动”的主动防御局面，让攻击者“无路可走”。本文聚焦于如何帮助企业从规划、建设到应用各个阶段建立一套成熟、可靠、科学的威胁情报能力。同时针对最重要的情报质量评估领域给出了一套科学的评估方法，并针对入侵类和失陷类场景给出了实践案例，包括基于 SOAR 的自动化威胁处置案例，为其他计划构建威胁情报能力的组织提供建设和应用探索。

参考文献：

[1] CNCERT/CC. 2016 中国移动互联网发展状况及其安全报告[R]. 2016.
CNCERT/CC. China mobile Internet development and security report[R]. 2016.

[2] 孙增. 高级持续性威胁(APT)的攻防技术研究[D]. 上海: 上海交通大学, 2015.
SUN Z. The attack and defense technology research of advanced persistent threat[D]. Shanghai: Shanghai Jiao Tong University, 2015.

[3] TOUNSI W, RAIS H. A survey on technical threat intelligence in the age of sophisticated cyber attacks[J]. Computers & Security, 2018, 72: 212-233.

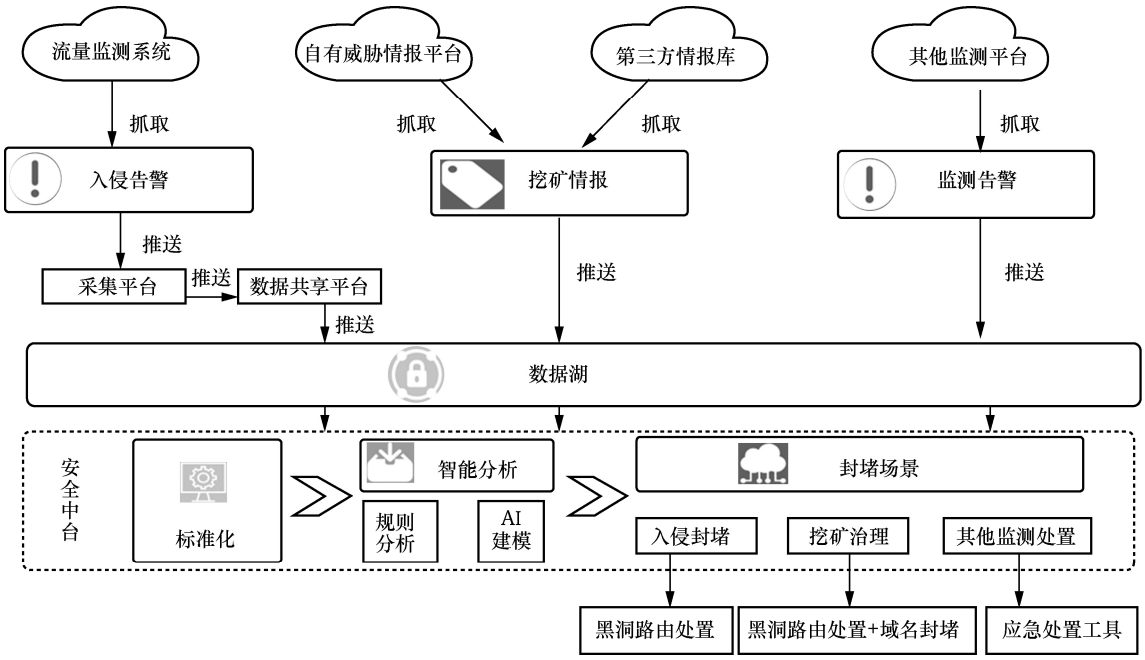

图 5　基于威胁情报的自动化威胁处置响应

[4] 左晓栋. 立法困局下的战略新部署: 美国关键基础设施保护行政令述评[J]. 中国信息安全, 2013(3): 74-75.
ZUO X D. New strategic deployment in the legislative dilemma: a review of the U.S. executive order for critical infrastructure protection[J]. China Information Security, 2013(3): 74-75.
[5] 赵艳玲. 浅谈美国《提升关键基础设施网络安全框架》[J]. 信息安全与通信保密, 2015(5): 16-21.
ZHAO Y L. A brief talk on “framework for improving critical infrastructure cybersecurity”[J]. Information Security and Communications Privacy, 2015(5): 16-21.
[6] 宋国涛. 试析美国《网络安全信息共享法案》[J]. 保密科学技术, 2016(6): 28-31.
SONG G T. Analysis of the US cybersecurity information sharing act[J]. Secrecy Science and Technology, 2016(6): 28-31.
[7] NIST. SP800-150: guide to cyber threat information sharing[S]. 2014.
[8] 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(8): 86-91.
WANG Q X, YANG W. Extraction of threat intelligence entities based on STIX[J]. Cyberspace Security, 2020(8): 86-91.
[9] CASEY E, BACK G, BARNUM S. Leveraging CybOX™ to standardize representation and exchange of digital forensic information[J]. Digital Investigation, 2015, 12: S102-S110.
[10] USSATH M, JAEGER D, CHENG F, et al. Pushing the limits of cyber threat intelligence: extending STIX to support complex patterns[C]//Information Technology: New Generations. [S.l.:s.n.], 2016.
[11] FRANSEN F, SMULDERS A, KERKDIJK R. Cyber security information exchange to gain insight into the effects of cyber threats and incidents[J]. Elektrotechnik und Informationstechnik, 2015, 132(2): 106-112.
[12] 林玥, 刘鹏, 王鹤, 等. 网络安全威胁情报共享与交换研究综述[J]. 计算机研究与发展, 2020, 57(10): 2052-2065.
LIN Y, LIU P, WANG H, et al. Overview of threat intelligence sharing and exchange in cybersecurity[J]. Journal of Computer Research and Development, 2020, 57(10): 2052-2065.
[13] 杨沛安, 武杨, 苏莉娅, 等. 网络空间威胁情报共享技术综述[J]. 计算机科学, 2018, 45(6): 9-18, 26.
YANG P A, WU Y, SU L Y, et al. Overview of threat intelligence sharing technologies in cyberspace[J]. Computer Science, 2018, 45(6): 9-18, 26.
[14] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 网络安全威胁信息格式规范: GB/T 36643—2018[S]. 2018.
State Administration for Market Regulation, Standardization Administration. Information security technology—cyber security threat information format: GB/T 36643—2018[S]. 2018.

[作者简介]

张海涛（1983– ），男，中国移动通信集团浙江有限公司网络安全部高级工程师，主要研究方向为威胁情报、态势感知、5G 安全等。

蒋熠（1981– ），男，中国移动通信集团浙江有限公司网络安全部主管，主要研究方向为威胁情报、5G 安全、零信任、态势感知。

竺士杰（1978– ），男，中国移动通信集团浙江有限公司网管中心副主任，主要研究方向为威胁情报、5G 安全、零信任、态势感知。

陈琦（1990– ），男，中国移动通信集团浙江有限公司网络安全部工程师，主要研究方向为威胁情报、态势感知、5G 安全等。