Computer Science and Application 计算机科学与应用, 2019, 9(10), 1939-1945
Published Online October 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.910217

Hans汉斯

Research on Application of Threat Intelligence in Situational Awareness

Jilei Li, Zhiqi Jiang*

Country First Research Institute of the Ministry of Public Security, Beijing
Email: 578162586@qq.com, *jzqtw@foxmail.com

Received: Oct. 2nd, 2019; accepted: Oct. 17th, 2019; published: Oct. 24th, 2019

Abstract

As the priority of cyber-security arises world-wide, network security situation awareness (NSSA) and its application are receiving more attention from researchers. High-quality threat intelligence can greatly improve the efficiency of detection, analysis and emergency response which change the offensive and defensive posture. This paper introduces the concept of situational awareness and threat intelligence, and then discusses the specific application scenarios of threat intelligence in situational awareness. The research results show that it will play a greater role in situational awareness with the development and maturity of threat intelligence technology.

Keywords

Network Security Situation Awareness, Threat Intelligence, Security Warning

威胁情报在态势感知中的应用研究

李际磊，蒋志颀*

公安部第一研究所，北京
Email: 578162586@qq.com, *jzqtw@foxmail.com

收稿日期：2019年10月2日；录用日期：2019年10月17日；发布日期：2019年10月24日

摘　要

随着网络空间安全重要性的不断提高，网络安全态势感知(network security situation awareness，简称NSSA)的研究与应用正在得到更多的关注。高质量的威胁情报可以大幅度地提升检测、分析、应急响应效率，进而改变攻防态势。本文介绍了态势感知和威胁情报的概念，研究了威胁情报在态势感知中具

*通讯作者。

文章引用: 李际磊, 蒋志颀. 威胁情报在态势感知中的应用研究[J]. 计算机科学与应用, 2019, 9(10): 1939-1945.
DOI: 10.12677/csa.2019.910217

体的应用场景。研究结果表明随着威胁情报技术的不断发展成熟，其将会在态势感知中发挥更大的作用。

关键词

网络安全态势感知，威胁情报，安全预警

1. 引言

随着网络威胁呈泛化和持续化趋势发展，多样化的攻击切入点、高水平的入侵方式、系统化的攻击工具使网络威胁代价降低。根据国家互联网应急中心(CNCERT)于 2019 年 4 月 16 日发布的《2018 年我国互联网网络安全态势综述》[1]可知，在 2018 年我国网络安全法律体系进一步健全、网络安全管理体制进一步完善和公共互联网网络安全监测和治理进一步加强的情况下，关键基础设施等面临的风险依旧突出，APT 攻击、DDos 攻击等问题依旧较为严重。

为最大限度地保护核心系统资产安全，需对传统的安全防御方式进行优化和改进，形成能应对多样化和持续化威胁的安全体系。在此背景下，网络安全态势感知需要融入新的技术，更加有针对地对关键信息基础设施或特定目标进行多方位要素信息获取、智能分析以及态势预测，从而切实保障网络安全，实现“全天候全方位网络安全态势感知”的目标。

由于高级网络威胁攻击的普遍化，威胁情报近两年在全球市场呈爆发趋势，这是大数据发展应用之后的一种必然现象，是网络安全领域追求智能化、高效率的基本诉求与大数据情报搜集与应用能力相互反馈和完善的结果。威胁情报能够提供关于某攻击事件或黑客组织的重要特点与关键信息，能够为中高层安全管理人员的安全防御决策、安全策略制定提供重要的参考，并促进安全事件的快速预警与响应，为全面感知网络安全态势提供重要的数据支撑。

本文主要对威胁情报在态势感知中的应用场景进行研究，第 2 节给出态势感知和威胁情报的概念，第 3 节讨论威胁情报在态势感知中具体的应用场景，第 4 节对全文进行总结。

2. 相关概念

2.1. 网络安全态势感知

网络安全态势感知的最早定义是 1995 年由 Endsley [2]提出，认为“态势感知是指在一定时空条件下，对环境因素的获取、理解和对未来的预测”，也就是说，态势感知首先需要通过一定方法获取过去与当前的各类环境要素，然后通过分析与研究从环境要素中有所“感知”，从而对未来态势的发展有所预测。2010 年，Springer [3]等人再次给出更加细化的定义，认为“网络空间(防御)态势感知涵盖态势识别、态势理解和态势预测三个阶段，至少包括 7 个方面的内容：态势认知、攻击影响评估、态势跟踪、对手趋势和意图分析、态势因果关系与取证分析、态势信息质量评估、态势预测”，这一定义中包含了态势感知具体工作的流程与技术七个方面，这七方面概括起来又可归纳为三个层面，即“态势识别”、“态势理解”和“态势预测”[4]。

2.2. 威胁情报

威胁情报的定义随着时代和技术的发展逐步演进[5]。2013 年美国 IT 咨询公司 Gartner 对威胁情报作了较为权威的定义：“威胁情报是一种基于证据的知识，它就网络资产可能存在或出现的风险、威胁，给出了相关联的场景、机制、指标、内涵及可行的建议等，可为主体响应相关威胁或风险提供决策信息[6]。”此外，还有国内学者[7]提出“威胁情报是通过大数据、分布式系统或其他特定收集方式获取，包括漏洞、威胁、特征、行为等一系列证据的知识集合和可操作性建议”。

本文选取 Gartner 对威胁情报的定义，并且将实际应用中的威胁情报分为三个层面：一是数据层面，例如基础的域名、IP、证书、CVE 信息等，这一层面的情报一般数量巨大，但仅仅是最基本的数据采集的结果，研究和分析人员并不能从中直接得到具有指导性的信息；第二层是信息层面，是在数据层面情报的基础上，通过数据的统计、关联分析与可视化，得到事件或攻击组织层面的具有一定指导意义的情报信息，例如黑白名单、关于恶意域名/IP 的地域统计分布等；第三层面是知识层面，是在信息层面情报的基础上，再进行深层的多源异构数据关联分析，得到对某一攻击事件或某一黑客组织的较为完善的分析报告，并且在一定程度上含有对未来安全态势的分析和预测，提出较具有参考价值的安全防护建议等。

3. 威胁情报在态势感知中的应用

威胁情报是态势感知所依据的重要资源，基础威胁情报数据往往数量庞大，这为基于机器学习和深度学习方法安全智能化提供了基础数据源[8]。其应用核心是数据、重点是分析，大量威胁情报数据经过挖掘分析后产生的攻击详细信息(攻击是否已知、攻击意图、攻击手法、攻击目标、如何排查等等)可以使防护方因势而动、制定更有效的防护策略，做到“上医医未病之病”，将安全风险拒之门外。能够驱动态势感知系统进行及时且准确的响应，正是威胁情报的价值所在。

3.1. 基本应用环节

如图 1 所示，威胁情报在态势感知中的应用可总结为四大环节：

预测环节。通过分析战术类威胁情报中攻击事件、恶意样本、漏洞等信息，评估当前系统面临的风险，预测其可能遭受的攻击行为，划定安全事件响应基线。

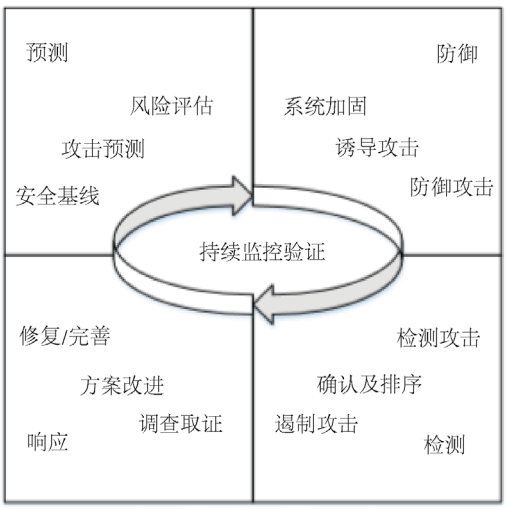

Figure 1. The basic application of threat intelligence in situational awareness
图 1. 威胁情报在态势感知中的基本应用环节

防御环节。在预测完成后、攻击来临前，需加固系统防御措施，必要时可实施诱导攻击等攻击性防御手段。

检测环节。通过比对操作类威胁情报中 IP 信誉、文件信誉及其他指纹特征，尽可能全面地检测系统中的异常动向，及时确认攻击行为并按优先级排序，采取相应手段遏制。

响应环节。检测、遏制攻击后要及时调查成因、留存证据，并根据攻防对抗过程和攻击造成的影响改进前三个环节的方案，修复和完善安全防护系统。

3.2. 基于用户角色的不同应用场景

态势感知中有关威胁情报的应用对不同用户有不同的价值[9]：

对于需要安全防护的企业，威胁情报应用于态势感知可以大大缩短从威胁检测到应急响应的时间周期；还可以帮助管理层对下级子公司或者分支机构进行管理，对安全预算、安全流程改进、安全人员配置做出更好的决策，同时全方位、快速了解行业内的安全状况；

对于监管、风险控制和应急响应部门，威胁情报应用于态势感知可以提供对监管对象和供应商网络安全状况评价的客观依据；

对于负责基础设施安全保障的日常安全运维人员，他们在安全事件处理过程中，可以利用威胁情报所提供的恶意软件签名、黑名单等数据对事件进行辅助判断，决定防火墙、网关、IDS/IPS 系统和其他安全产品是否采取阻断控制；

对于网络安全专家，他们需要有关攻击者和攻击行为的深入情报，即描述敌手的战术、技术和程序(TTP)的“战术情报”，进行有关恶意软件分析、目标漏洞成因的专业技术分析，提高安全服务能力。

3.3. 基于特定需求的不同应用场景

即使是同一类用户，在态势感知中使用威胁情报的具体需求也不尽相同，威胁情报在这些特定需求下的应用场景包括：安全预警、实时对比研判、历史回溯、交互式威胁猎捕、协同响应、情报机读化、攻击背景分析等。

3.3.1. 安全预警

安全预警是网络空间安全态势感知的第一道防线，完备的预警机制可以让安全运维达到事半功倍的效果，是在安全对抗中掌握主动的关键。如果不能居安思危、敏锐地捕捉到当前系统中可能存在的风险，那么对安全事件的检测、响应和处理就更无从谈起。安全预警通常包括对潜在威胁的预警、对系统漏洞的预警和对攻击事件的预警，如图 2 所示。

(1) 威胁预警

攻击情报(战略情报/战术情报)被收录进攻击情报库，给出了宏观层面的攻击背景、攻击者有关情况以及攻击目标、攻击实施流程等细节，这些描述与漏洞库中漏洞危害级别、漏洞类型(将如何被攻击者利用)等信息进行比对，决定是否触发威胁预警。例如，通过威胁情报的采集与分析，发现某组织对某能源企业进行持续性攻击：攻击情报与攻击情报库的匹配结果显示攻击者具体采用的是钓鱼邮件类的攻击手段，利用嵌入到邮件正文中的链接或附件中的恶意代码攻击系统漏洞；该结果再次与漏洞库进行匹配，显示这类攻击利用的漏洞是零日漏洞，特征明显、证据完备，于是触发威胁预警。

(2) 漏洞预警

首先将收集到的漏洞类威胁情报信息与漏洞库进行比对，一旦命中某类漏洞，再将漏洞库中该类漏洞的厂商、受影响实体等信息与资产库中系统、应用、相关组件的名称和版本等信息进行比对，若匹配到结果则触发漏洞预警。

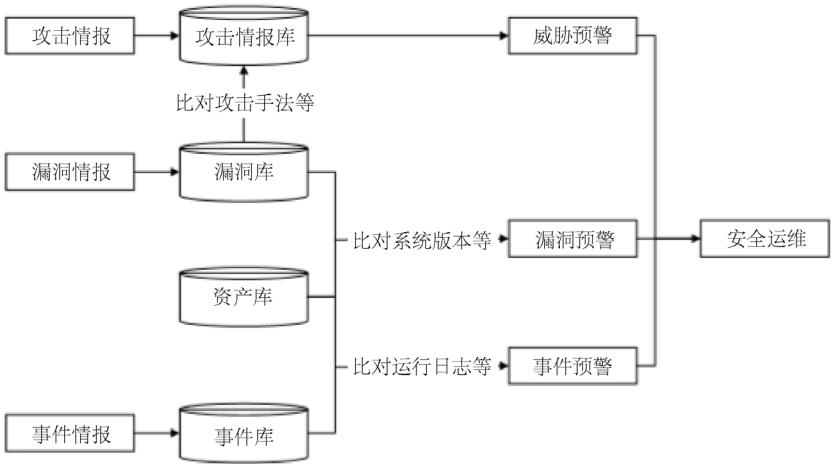

Figure 2. Schematic diagram of security warning process
图 2. 安全预警流程示意图

(3) 事件预警

事件情报的来源多、内容涉及广，在大量的内部和外部事件中发现两起甚至多起事件的关联是事件预警的前提。例如，详细分析事件情报发现，某单位互联网出口中一些通信设备产生的流量是与 C & C 服务器通信的流量，同时有从暗网中得来的威胁情报表明，该单位的敏感信息在暗网黑市中被售卖，两起事件对应到一起触发了事件证据完备，触发事件预警。

3.3.2. 实时比对

信息从来都是并将一直是安全决策的关键因素。攻防双方在信息时效性和有效性上的差距几乎意味着实力的差距和竞争的胜负。因此威胁情报常与时效性高的实时数据结合，作为重要的参考条件筛选出更加有效或是针对某一特定关注点的信息资源，使防护方掌握“新”、“准”兼备的网络安全态势。

持续采集网络状况、主机行为等实时事件流的入侵检测系统往往会产生大量告警，但其中有相当一部分告警是误告警，这些误告警不仅白白地消耗了防护平台的安全事件响应和处理能力，更严重的是其引发的错误安全决策可能影响受保护客户的正常业务。如果以威胁情报库作为比对依据，在实时事件流触发事件告警之前，在实时关联引擎中按照定义好的情报关联规则确认某事件是否足够可疑到被视为威胁情报，例如若某攻击源处在确定性置信白名单中，则取消该告警，那么可以消除大量无效告警，减轻后续安全运维与分析的压力。

在反欺诈检测中，防护方一般更加关注账号的异常行为。首先持续搜集某可疑目标的所有实时数据，再与恶意 URL、恶意域名、恶意 IP、域名解析库等威胁情报信息比对，将关注点聚焦在“平均一个异常 IP 使用两次”、“失陷账号平均使用少于 5 次”等异常行为，由这些行为特征生成置信度不同的告警。例如，可以设置“1 分钟内，来自同一个源的 WEB 请求数量大于预定义的阈值，并且源 IP 在威胁情报中命中了高威胁度 IP”作为情报关联规则，一旦规则命中，立即触发高置信度告警。另外，在产生并记录告警后，还可以对该 IP 添加威胁情报标签，对威胁情报起到反馈作用。

3.3.3. 历史回溯

历史回溯是基于新的外部共享知识对旧的内部审计记录进行查漏补缺的过程。任何防护系统都不是无懈可击的，总会有精心伪装的攻击者成为漏网之鱼，但由于现阶段威胁情报的大规模共享，我们从接收到的外部威胁预警情报中很有可能发现这些自己遭受过却浑然不觉的攻击。例如，如果从来自某安全组织的外部情报中发现自某个时间点起，该组织掌握了一组用于信息窃取操作的僵尸网络的 IP 地址，那

么可以回溯本单位从该时间点起至今所形成的内部告警库/事件库，查看是否有来自这组僵尸网络的 IP 地址的访问记录，并基于连接具体行为和处理情况，判断影响、评估造成的损失。虽然这种方式多少有些“亡羊补牢”的意味，但这些重新被审计的攻击行为将作为强特征，成为对今后决策依据的重要补充。

3.3.4. 威胁猎捕

威胁猎捕是对威胁进行详细分析并试图反制的过程，其中威胁情报可以提供多个层面的线索支撑。第一阶段，与实时比对类似，系统根据攻击情报库、安全事件库和情报关联规则，从实时事件流日志或告警中发现蛛丝马迹，判定其中的事件是否为可疑事件，对可疑事件从攻击来源和攻击目标两方面展开持续、细致的侦查：a) 确定系统内部受到攻击影响的目标，对该受害目标持续跟踪监测、挖掘分析所得数据，生成有关该目标资产信息的内部情报，同时还原完整的攻击链，展示攻击过程和手法；b) 对外找到直接的攻击源，结合通过共享得来的外部安全情报库，尝试寻找攻击源存在的漏洞，实现反制，并逐步找出攻击实施人员，甚至发现幕后的组织。整个过程中威胁情报在内部事件关联和外部攻击溯源两大环节中都发挥了关键作用，如图 3 所示。

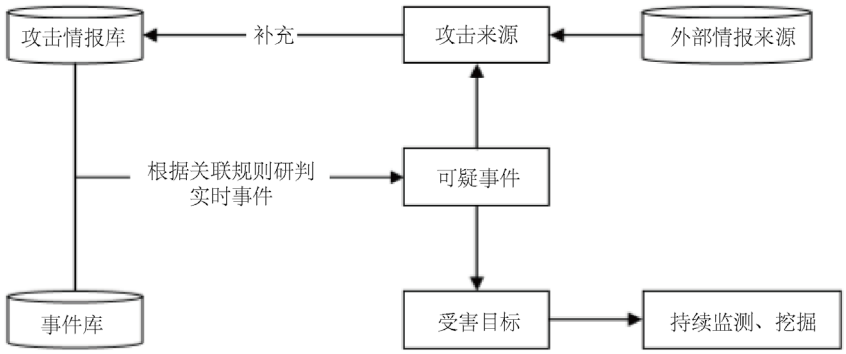

Figure 3. Threat hunting process diagram
图 3. 威胁猎捕流程示意图

另外，系统生成的内部安全情报除了用于补充自身的攻击情报/安全事件库，也可以共享或是进行商业化交易，成为其他安全系统追踪攻击源时依据的外部安全情报库。如在政府或非营利部门内，不同机构在威胁猎捕中生成的内部威胁情报可按照一定的政策机制(如政务信息资源共享)进行情报的共享；营利机构与非营利机构、营利机构之间可通过情报服务供应商进行威胁情报交易，也可通过约定好的协议或标准进行协同。

3.3.5. 协同响应

协同响应是威胁情报在态势感知中的重要应用形式。如今的安全系统为了应对日益复杂的攻击手段，往往规模庞大、构造复杂，包括由防火墙、IDS 等组件组成的安全设备系统和由内部人力手动操作进行配合的运维系统，而协同响应的目标是使这些子系统成为一个有机整体，在安全事件响应和处理过程中步调一致。这就需要以外部及内部威胁情报为基础，在对事件做出研判决策后，将事件信息与内部资产信息进行匹配，对匹配到的相关设备给出指令，如为防火墙配置 ACL 规则阻断某些连接等，实现设备间的联动，同时利用工单系统、OA 协同系统或邮件/短信/微信等多种形式的协同请求，对相关人员给出指令，如手动执行打补丁、升级病毒库等操作或进行其他安全配置，实现人与设备的联动。

4. 总结

在大数据、云计算、物联网等新型信息技术飞速发展的背景下，网络空间威胁也向朝泛化和复杂化

的趋势发展，各类网络攻击也更加具有持续性和隐蔽性。基于威胁情报进行网络安全防御能够及时分析已发生的入侵，对未来威胁态势进行预判，并据此评估潜在的安全风险以指导用户制定有效的安全决策，系统化增强网络空间防御能力。本文通过分析威胁情报在态势感知中的基本应用环节，探讨了威胁情报对于需要安全防护的企业、风控与应急响应部门、日常运维人员和网络安全专家等不同角色人员的应用；基于特定需求，介绍了威胁情报在典型场景中的应用流程。随着威胁情报技术的不断成熟及相关规范、框架的日渐完善，在安全问题日益严峻的未来，它将进一步在社会、国家乃至全球的各个层面发挥巨大的作用。

参考文献

[1] 中国互联网应急响应中心. 2018 年我国互联网网络安全态势综述[Z].

[2] Endsley, M.R. (1995) Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, **37**, 32-64. https://doi.org/10.1518/001872095779049543

[3] Tadda, G.P. and Salerno, J.S. (2010) Overview of Cyber Situation Awareness. In: Jajodia S., Liu P., Swarup V. and Wang C., Eds., *Cyber Situational Awareness*, Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-0140-8_2

[4] 单琳. 网络威胁情报发展现状综述[J]. 保密科学技术, 2016(8): 28-33.

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

[6] 林晨希, 薛丽敏, 韩松. 浅析网络安全威胁情报的发展与应用[J]. 网络安全技术与应用, 2016(6): 12-13.

[7] 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(3): 1-12.

[8] 2017 安全分析与情报大会. 微步在线-薛锋: 基于威胁情报的安全智能化[R].

[9] 2017 安全分析与情报大会. 谷安天下-赵毅: 威胁情报正在和企业安全架构全面融合[R].