2022 IEEE 第十届联合国际信息技术与人工智能会议(ITAIC) - 978-1-6654-2207-9/22/$31.00©2022 IEEE - DOI: 10.1109 / ITA

基于人工智能的网络攻击信息获取与监控方法研究

闫磊，刘新锐，杜春辉，裴俊杰
国网甘肃电力公司兰州 yanleirty@163.com, 982157601@qq.com, 15002637533@163.com, peijunjie18@163.com

网络空间是继陆、海、空、天之后的第五大活动空间。维护网络空间安全是事关国家安全、国家主权和人民合法权益的重大问题。随着人工智能技术的快速发展及其在各个领域的应用，网络空间安全面临着新的挑战。 如何帮助网络安全人员随时掌握安全趋势，帮助网络安全监控人员快速响应告警信息，便于监控人员的跟踪和处理。本文介绍了一种利用态势感知微应用实战攻防机器人将网络攻击信息快速反馈给监控人员，将攻击信息及时上报给信息上报平台，自动拦截恶意 IP 的方法。

关键词:网络攻击;信息获取;监测方法;人工智能

I. 介绍

如今，移动互联网、云计算、大数据、物联网、人工智能正在蓬勃发展。他们不断地跨界整合各种垂直产业。各种新技术、新应用层出不穷，信息安全和网络安全问题日益突出。随着人工智能新技术的普及和应用，黑客开始利用人工智能进行网络攻击，这不仅扩大了黑客的攻击面，也让黑客拥有了更多的攻击手段。面对利用人工智能的黑客攻击，最好的防御策略是利用人工智能和新的安全架构。原因有二:一是随着网络攻击的增多，危害程度加大，网络安全专业人才严重短缺。其次，“零日攻击”等新形式的攻击有所增加，使得防范变得更加困难。在网络安全的日常运维中，特别是在保障期内，判断 IP 地址、攻击时间、攻击方式、攻击次数、被攻击是非常重要的对外部网络的设备等信息攻击者更加快速准确，反应迅速。本文将介绍一种利用态势感知微应用实际攻防机器人将网络攻击信息快速反馈给监控人员，将攻击信息及时上报给信息上报平台，自动拦截恶意 IP 的方法。

II. 实施背景

在网络安全攻防演练和保障期间，监控人员通常需要 24 小时同时关注不同的监控溯源平台，进一步分析新出现的威胁，并及时撰写快递报告和报告。工作任务很重。

同时，监控人员在经过长时间的工作后，始终保持着高度集中的状态，这必然会导致放松和注意力不集中。特别是在攻防演练中，需要通过信息上报平台及时上报攻击者的信息和被攻击设备的信息。攻击前，攻击者通常会扫描被攻击设备的端口和漏洞，导致溯源监控系统上报大量攻击信息，大大增加了监控人员的工作压力。

此外，传统的网络安全分析监控处置的工作模式是“发现异常(安全设备报警)→分析判断(人工分析)→事件处置(阻断攻击源 IP /处置资产)”。整个工作过程耗时较长，对保安人员的个人能力要求较高。当调度员在夜间值班时，处理工作更难完成。

综上所述，有必要充分利用协同防御和联动处置技术，构建一个基于安全调度能力的自动化运维平台，提供安全保障

安全运营能力，以自动化编排为核心，汇聚搭建不同场景，为前端业务运营提供定制化安全服务，实现“整合安全资源组件，沉淀安全业务场景”，为安全服务的快速交付和运营提供服务，降低人工风险排查成本，找到帮助网络安全监控器快速响应报警信息的途径;深化安全防范，构建智能主动的立体安全防护体系。

微眼应用完成后，第一版公司态势感知降噪已上报至第一版公司内部态势感知降噪，并通过第一版互联网对当前态势进行有效过滤。实现技术对技术、技术对技术的控制，确保公司网络在严峻形势下安全稳定运行。

A. 基础数据管理

通过 syslog、WebService 独立采集等数据访问方式，实现对现有各监控子系统的数据采集，整合相应的安全能力，对数据进行采集、删除和规范化，实现对现有基础数据的治理，验证数据的有效性和完整性，实现“一个数据源”。

B. 有效设备和有效数据的汇总和分析

通过对现有数据源按功能类别进行区分，进行时间序列分析、统计分析、聚类分析、场景分析等维度，并为安全人员提供用户自定义的关联分析窗口，及时调整分析模型，将海量不相关的报警数据合并为攻击事件，减少安全人员在事件分析过程中所花费的精力。告警数据和数据取证。

C. 事件预警和智能联动

在事件发生时，通过与防火墙的智能联动联合防御，自动识别攻击源的攻击入口，自动识别正在使用的阻断节点设备的阻断路径和工作状态，对点对点的攻击源进行 IP 阻断，从而实现对攻击源 IP 地址和恶意攻击(秒内多次攻击，攻击规则复杂;等等)。随后，通过漏洞预警平台，进行漏洞处置和控制，并实时反馈修复状态。

内部业务应用系统。该功能使用实际的攻防机器人程序将提交的攻击 IP 以特定的格式记录和存储，然后将这些 IP 地址发送到 FTP 服务器。Netshield 系统会定期在 FTP 服务器中自动识别这些 IP 地址，加入情报库并进行拦截。

C. 开发和应用攻击监测的自动处置工具。

结合现有安防设备的报警进行数据采集、权重配置、攻击源与攻击类型、过滤、降噪和综合分析，结合内外威胁情报与报警条件的相关性分析实现攻击源 IP 的准确分类。与深度威胁安全防护网关进行联合防御，结合 API 或联动工具下发阻断处置任务，自动识别正在使用的阻断节点设备的阻断路径和工作状态，进行点对点攻击源 IP 阻断，实现对攻击源 IP 地址和恶意攻击(秒内多次攻击、攻击规则复杂等)的自动发现和联动阻断。制定实际的攻防机器人程序，将提交的攻击 IP 以特定格式进行记录和存储，发送到网盾系统的情报基地进行拦截和拦截。随后，通过漏洞预警平台，开展漏洞处置控制工作，实时反馈修复状态，

III. 实现方法

目前，钉钉程序中携带的自定义机器人功能支持 Java 和 python 独立编程。在此基础上，结合态势感知平台和防御处置措施的分析结果，通过 API 将态势感知平台、钉钉程序和防火墙关联起来，构建自动化实战攻防机器人，实现报警信息的及时提交和恶意 IP 的自动处置。具体内容包括:

A. 用机器人程序监控攻击信息

用户在获取到群组的 webhook 地址后，可以向该地址发送 HTTP post request，实现了向群组发送消息的功能。因此，您只需要在办公室外联网计算机上下载并设置机器人客户端，编写实际攻防机器人程序，将态势感知微应用信息发送给机器人，然后由机器人发送到钉组即可。在机器人程序中设置要发送的报警级别、攻击次数阈值、钉钉机器人发送的组中要显示的内容。复制完成后，即可进行测试并投入使用。

B. 利用机器人程序处理攻击信息

向信息上报平台上报攻击信息。

如果需要向信息上报平台上报攻击信息，则需要设置实际攻防机器人向信息上报平台网站发送 HTTP post 请求，并设置格式和内容，完成信息上报功能。提交完成后，可以考虑设置将提交完成信息发送到钉组，提醒监控人员，也方便监控人员识别信息是否缺失或错误。

实现与防火墙设备联动，实现 IP 拦截。

通过防火墙调度引擎联动联合防御，结合 API 或联动工具下发封禁处置任务;自动识别攻击源所在的攻击入口，自动识别正在使用的阻断节点设备的阻断路径和工作状态，阻断攻击源的 IP;设置阻塞时间，不限于按小时/天/周的周期进行处理;可与值班工作的工单流程模块联动，以日/周/月为单位进行安全监控封禁 IP 表单;通过 NETCONF 接口协议开发防火墙接口，实现业务应用安全策略的自动发布和删除

实现网络安全监控信息集中、分析处置，形成网格网络安全预警处置机制和实时指挥机制。

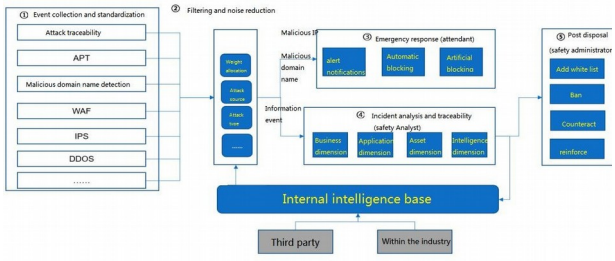

图 1 所示。攻击监控自动处置工具的体系结构。

图 2 所示。人工智能机器人平台

图 3 所示。机器人自动报告

IV. 应用场景

为了避免机器人发送大量的垃圾信息，美甲机器人每分钟最多只能发送 20 条信息。因此，为了提高

B. 夜班现场

夜班主要是指非再保险期的值班期，通常由调度员协助看守安全系统。其特点是:没有安全人员值班，很难在第一时间人工判断是否处理，需要根据不同的事件类型自动处理。

C. 再保险期方案

再保险期主要是指再保险期的值班期，以 24 小时安全人员值班为特征。针对不同类型的安全事件，结合封堵时间和封堵设备进行处理。

V. 实现的效果

通过测试和实际应用，网络安全分析室通过智能联动防御系统自动拦截大规模扫描攻击 890124 次，正向攻击 1746867 次，病毒、木马等反向外展 IP 地址 90156 次。采集安全设备报警信息，自动发送至钉组，对网络边界、终端、服务器、虚拟化等层面进行检测和阻断，创新网络安全态势监控平台、智能联动、全场景态势感知平台和自动攻击处置工具，自动准确定位安全事件根源，并快速判断、处置和恢复;全面支持公司信息系统安全稳定运行，提高应对网络安全的能力，为公司网络安全建设打下坚实的基础。

通过应用基于人工智能的网络攻击信息采集与监控方法，可以填补以往监控、分析、处置、跟踪和监控等非智能的空白

监控效果，进行了复位。当在实际应用中发现钉钉机器人每分钟提交大量攻击消息时，监控人员需要通过态势感知微应用、可追溯监控、WAF 等方式，验证在这段时间内是否存在信息缺失。同时，可以根据目前需要报道的信息平台类型对 applet 进行调试，构建一种适应当前主流报道平台的方式。此外，结合日常值班场景、夜间值班场景、再保险期场景设置不同的安全处置流程，实现智能联动处置，包括:

A. 日常工作场景

日常值班主要指安全人员在非再保险期间工作日的日常值班。其特点是:有安全人员值班，结合安全事件类型，可通过自动/手动判别处理。

跟踪全部是人工参与，提高了整个过程中处理安全事件的效率。建立联动机制后，可以有效摆脱“单兵作战”，建立安全生态系统，增加网络灵活性，最大限度地实现业务支持，在防御设备和分析设备之间进行实时联动，实时共享情报，让威胁无处可逃。当受到网络攻击时，安全设备能够快速响应，及时拦截病毒的传播，保证业务系统的正常运行，满足合规性要求，有效监控和预防，使信息管理者比以往更加了解系统中的所有信息和系统的健康状况，变被动为主动，“抵御门外的敌人”。实现信息安全的提前预防、事件检测与分析、事件中快速响应、事后可追溯等全流程的智能化、自动化处置。做到有效预警、及时处置、有序回收、持续改进。

参考

[1] [6]项成成基于并行深度森林的网络安全态势预测方法研究与应用
[D]电子科技大学，2021。

[2] 杨义跃，付志波，肖晓分析电力系统网络安全架构[J]电子技术与软件工程，2020 (22): 247 - 248

[3] 邓涛供电公司信息安全防护技术方案研究[J]通信电力技术，2020,37 (11): 154 - 156。

[4] 熊申铎基于区域能源互联网的电力监控系统信息保护研究[D]华北电力大学(北京)，2019。

[5] 基于机器学习的电力工业控制网络异常流量检测技术研究[D] .上海交通大学，2019。

[6] 康文杰基于信息物理融合的智能电网鲁棒性分析及安全新模型研究[D] .国防科技大学，2018。