AI 态势感知在重大网络事件应对中的应用探索

彭俊玮¹ 张志豪² 谭开宇³ 田沁鑫⁴ 姬云豪⁵

1 汇安云信息科技有限公司 2 潍坊市公安局奎文分局 3 宜宾凯翼汽车有限公司

4 电子科技大学公共安全研究中心 5 成都工业学院网络安全研究实验室

DOI:10.12238/acair.v2i3.8592

[摘要] 文章探讨了基于人工智能的态势感知系统在重大网络事件中的实战应用价值,针对传统安全机制在应对新型网络攻击时的滞后性,提出AI态势感知系统通过深度学习、机器学习和大数据分析技术,实现了网络环境的全面实时监控。AI态势感知系统能将复杂安全数据可视化,辅助即时决策;利用机器学习自动处理异常,减负人工;并可以瞬时响应威胁,动态调整防护策略。实战案例展示了系统在一分钟内识别并应对APT攻击的能力,证明了其在提升响应速度、准确性和防御主动性上的显著优势。

[关键词] 人工智能; 重大网络事件; 实战应用; 智能预警; 网络安全防护

中图分类号: TN915.08 **文献标识码:** A

Application of AI situational awareness in response to major network incidents

Junwei Peng¹ Zhihao Zhang² Kaiyu Tan³ Qinxin Tian⁴ Yunhao Ji⁵

1 Hui'an Cloud Information Technology Co.,LTD 2 Kuiwen Branch, Weifang Public Security Bureau

3 Yibin Kaiyi Automobile Co., LTD

4 Public Safety Research Center, University of Electronic Science and Technology

5 Network Security Research Laboratory, Chengdu University of Technology

[Abstract] This paper discusses the practical application value of artificial intelligence-based situational awareness system in major network events. In view of the lag of traditional security mechanisms in dealing with new network attacks, it is proposed that AI situational awareness system realizes comprehensive real-time monitoring of network environment through deep learning, machine learning and big data analysis technology. AI situational awareness system can visualize complex security data to aid immediate decision making. Use machine learning to automatically deal with anomalies and reduce labor burden; In addition, it can respond to threats instantaneously and dynamically adjust protection policies. The combat case demonstrated the system's ability to identify and respond to APT attacks within one minute, demonstrating significant benefits in improving response speed, accuracy, and defensive initiative.

[Key words] artificial intelligence; Major cyber incidents; Practical application; Intelligent early warning; Network security protection

前言

当数字化转型浪潮涌动,互联网基础设施的深化普及与信息交互复杂度的飙升,为社会进步铺设道路之际,亦不可避免地诱发了网络空间安全威胁的指数级增长,这对国家安全、社会秩序及个体隐私权益构成了复合型挑战。传统安全防护机制,受限于规则预设与签名匹配的框架,面对APT等进化迅速、手段多变的新型网络攻击,暴露出预警与应对的滞后性,显得力有不逮。

在诸如勒索软件大规模爆发、国家关键基础设施遭受攻击等重大网络事件中,基于AI的态势感知系统展现出了卓越的实战价值。它能够在浩瀚的数据海洋中迅速捕捉到异常信号,利用

算法模型的智能分析,准确区分正常活动与恶意行为,为决策者提供及时、准确的情报支持,有效缩短了从威胁发现到响应处置的时间差,最大限度地减少了损失,保障了网络环境的安全稳定。

1 态势感知概述

态势感知是一种先进的网络安全监控与管理理念,通过集成高级数据分析、机器学习及实时监测技术,为组织提供对其网络安全环境的全面、实时且深入的理解^[1]。态势感知不仅仅局限于识别和响应已知威胁,更侧重于预测未知风险、理解网络行为模式并优化整体安全策略。

1.1 数据可视化

数据可视化构成了态势感知平台的核心能力,它将纷繁复杂的网络安全数据转化成一目了然的图表及仪表盘界面,为安全运维人员开辟了一条透彻审视网络环境安全态势的窗口^[2]。此功能的核心价值在于其显著降低了安全数据分析的复杂度,使不具备深厚安全背景的管理层亦能迅速全面地掌握安全状态,及时辨识隐患。

态势感知平台通常融合多元数据来源,涵盖网络流量日志、系统事件记录、终端行为日志、威胁情报等,通过实时收集、净化处理及深度关联分析这些信息,构建出多角度的安全视角。这些可视化工具不仅加速了安全团队的问题发现与应对过程,同时也为策略修订和资源合理配置提供了可靠的科学依据。

1.2 响应智能化

随着人工智能技术的持续演进,态势感知平台的智能化响应特性愈发显著,旨在运用自动化或半自动化的技术手段,加速并精确化安全事件管理流程,大幅度减轻人工介入的需求,以实现高效且精准的威胁应对策略^[3]。

结合人工智能技术的态势感知系统采用机器学习算法,深入挖掘累积的数据样本,通过深度学习机制自动辨认异常行为模式,对安全事件进行即时分类,拟合攻击事件模型,精确区分实际威胁与告警误报从而精简分析工作量。企业原本的威胁情报结合公开资料 and 实际数据采样搜集为态势感知平台提供丰富的历史事件数据库与最新的网络环境监测信息,使其能自动生成风险评估报告和具体的对策指导,为运维团队处置和应急安全事件提供强有力的支持。平台能够模拟实施不同应对策略的潜在影响,为决策层推荐最佳行动方案。在特定情境下,依据预设的应急规则,平台能自主执行响应操作,譬如隔离感染终端、阻断恶意流量路径,确保在第一时间控制住威胁扩散趋势,有效控制损害范围。智能化响应极大提升了应急处理的速度与效能,促使安全专家能够专注于更具挑战性与战略意义的安全管理活动,充分体现了人机协作的高效模式。

1.3 防护即时化

防护即时化代表了态势感知平台应对安全挑战的前沿理念,旨在构建一个能够瞬时响应并适应威胁态势的动态防御生态系统^[4]。此核心价值嵌入于平台之中,确保面对任何安全威胁都能迅速启动保护措施,将潜在损害降至最低,其关键在于平台实时监控的敏锐度与策略应变的灵活性。平台不间断地巡视网络环境的每个角落,从数据包的微小波动到系统日志的解析分析。一旦捕捉到异常行为、符合IOC指标的敏感流量及已知威胁的存在,立即进行威胁告警,确保安全团队获得即时通报,得以迅速介入,把握处置的黄金时机。

平台不仅是一部高效的监测机器,也是智能策略的策源地。它依据最新的威胁情报与网络动态,灵活调适安全防护策略。这意味着对高风险区域加强准入控制,或是依据最新威胁向量动态调整防火墙策略,确保防护网始终与瞬息万变的威胁手段和来源同频共振。特别是在架构庞大、网络结构复杂的组织中,

态势感知平台发挥着桥梁与指挥塔的双重角色。

2 AI驱动的态势感知系统的技术框架

在当今高度数字化的社会环境中,网络安全态势感知系统已逐步成为保护网络空间免受恶意攻击、确保数据安全和维护业务连续性的关键工具。AI(人工智能)态势感知系统作为这一领域的前沿技术,通过深度学习、机器学习、大数据分析等技术,实现了对网络环境的全面、动态、实时监控,有效提升了安全威胁的识别、分析和响应能力。

2.1 AI态势感知系统核心原理

AI态势感知系统通过融合人工智能的自动化学习与深度模式识别能力,对海量网络数据进行深度挖掘与高强度分析,旨在及时发现异常行为、预测未来安全挑战,并自主优化防御策略。系统运作流程始于多源数据的获取与预处理,利用传感器、日志审查及网络监控全方位搜集信息,并借助ETL技术净化、格式化数据,确保分析基础的准确可靠。随后,系统运用先进机器学习算法,利用BiLSTM等深度学习模型,配合精细的行为分析技术,深入挖掘数据中的安全威胁特征与用户行为模式,构建详尽的用户行为画像及系统交互模型。在此基础上,借助大数据处理能力,系统执行高级关联分析,实时监测并评估网络态势,识别异常活动,结合历史与实时数据预测安全风险。最终,通过直观的图形界面展示分析结果,为决策者提供易于理解的安全态势概览,加速安全决策过程,有效掌控网络安全大局。智能应对与主动防御体系:结合预设的防御策略与AI算法的即时分析反馈,本系统能够自主或在人为指导下执行高效防护操作,举措涵盖隔离受侵设备、拦截有害流量、优化安全协议等,实现了从反应式防护到预见性防御的战略升级,全方位加固网络安全防线。

2.2 关键技术层

在一个全面集成的态势感知平台中,数据捕获层级是所有层级的基础。通过布置在网络节点的智能探针和高灵敏传感器,结合Syslog、SNMP、JDBC等通讯协议,实现对网络流量信息、系统日志及关键事件记录的全面搜集。随后,数据预处理层级对原始数据进行净化,去除杂质、统一格式并调整一致性,确保数据质量,为后续深入分析提供坚实基础。数据仓储层级则利用Elasticsearch、MongoDB等高性能数据库技术,构建能够存储海量原始数据和分析成果的数据仓库中心,以支持PB量级的信息存储。在安全智能分析层级,利用机器学习和深度学习技术。最后,通过可视化展示与应用层级,将复杂的分析结论以直观的图表和仪表盘形式呈现,帮助决策者即时把握网络安全态势,快速制定应对策略。与此同时,响应协调与自动化层级与安全组件如防火墙、入侵防御系统等紧密集成,支持自动或人工触发安全策略执行,实现安全事件的无缝响应和高效联动,从而加固整个安全防护网络。

2.3 AI驱动的优势

AI驱动的态势感知相较于传统手段,展现出显著的优势与差异。传统方法依赖规则匹配与签名检测,对已知威胁反应迅速,但面对变异快、手法新颖的攻击则力有不逮。AI技术引入后,

系统能通过深度学习、机器学习算法自主学习网络行为模式,有效识别异常,乃至预测未知威胁。这不仅扩展了威胁检测的广度与深度,还大幅提升了响应速度与准确性。AI驱动下,态势感知能够智能化分析大数据,减少误报与漏报,同时借助自动化与智能化决策,优化资源分配,实现防御策略的持续迭代与优化,为网络安全防护提供了更为动态、主动的解决方案。

3 实战案例分析

在数字安全领域,应对日益复杂的网络攻击,特别是高级持续性威胁(APT)的挑战,已经成为安全行业的重大课题^[5]。传统的安全运营模式由于信息过载、技能要求高及人力资源限制,难以高效识别并应对隐蔽性强、技术先进的APT攻击。针对这一困境,360公司推出了一款创新的安全解决方案——360安全智能体(AI Agent),它利用先进的人工智能技术,实现了对APT攻击的智能化、自动化猎杀,标志着AI态势感知进入了智能主义新纪元。

360安全智能体基于360安全智脑大模型构建,整合了秒级响应的云端安全分析、万亿级别的大数据处理、实时威胁情报反馈以及全球实战攻防经验,旨在解决传统安全运营中告警繁多、真伪难辨及处置效率低下的问题。在某金融机构的实战案例中,360安全智能体展现了其一分钟完成APT攻击识别、溯源、分析及应对的卓越能力。

当一名财务人员不慎点击了伪装成PayPal账单的钓鱼邮件附件时,360安全智能体即刻通过其超越内核级的探针矩阵识别出潜在威胁,并迅速启动应急响应机制。该智能体首先对海量告警信息进行深度分析,有效过滤无关干扰,精准定位到与APT-C-28恶意服务器的通信告警,即时向用户发出紧急通知。随后自动调用威胁溯源引擎,依托集成的攻防对抗知识库,迅速追溯至攻击的源头——钓鱼邮件,根据IP分析,开放端口,判断是否为代理,从而进一步的去进行溯源反制,初步判断该IP为用户服务器的IP,进行端口扫描查看启动服务,并结合大数据模型在互联网上进行关键字关键词搜索,通过以上手段发现某端口搭建着钓鱼人员的XAMIND,进行自动反制,漏洞扫描,发现搭建socks平台NPS,存在逻辑缺陷进行绕过,在AI识别指纹和漏洞存在命令执行漏洞,从而进行了溯源反制,为后续响应提供了明确的目标。

由此可见,AI技术的引入,不仅极大地提升了安全运营的效

率和准确性,还降低了对高级安全专家的依赖,使得普通安全人员也能通过智能体的辅助,展现出如同专家般的处理能力。

4 结论

AI赋能的态势感知系统已经成为网络安全领域的一大突破,显著提升了对复杂网络攻击的预测和应对速度,为维护数字世界的稳定筑起了一道坚固的防线。以360安全智能体为例,其在无须人工干预的情况下,仅一分钟便能完成对APT攻击的精准识别、攻击溯源、链路绘制、威胁研判及资产分析等系列复杂操作,充分展示了AI技术在处理大量安全数据、实时监测异常活动、自动执行高级威胁狩猎方面的巨大潜力。这不仅极大提高了安全运营的效率,使得即使是普通安全人员也能基于AI辅助做出专业级别的响应,标志着安全防护正从被动防御向主动、智能化防御转型。

[参考文献]

- [1]杨宇,谷宇恒.网络安全态势感知综述[J].科学技术与工程,2022,22(34):15011-15019.
- [2]胡明亮.网络安全数据可视化综述[J].信息与电脑(理论版),2017(24):185-186.
- [3]王小鸿.基于大数据和人工智能技术的信息安全态势感知系统研究[J].大众标准化,2019,(14):18+20.
- [4]杨志琼,牟舵.珠江委网络安全态势感知平台设计与应用[J].水利信息化,2022,(02):16-20.
- [5]张瑜,潘小明,LIU Qingzhong,等.APT攻击与防御[J].清华大学学报(自然科学版),2017,57(11):1127-1133.

作者简介:

- 彭俊玮(2003--),男,汉族,四川省德阳市人,本科,网络工程师,研究方向:渗透安全工程师。
- 张志豪(2002--),男,汉族,山东省德州市人,专科,网络工程师,研究方向:渗透安全工程师。
- 谭开宇(2003--),男,汉族,四川省达州人,本科,通信工程师,研究方向:嵌入式设计。
- 田沁鑫(2002--),女,汉族,四川省成都市人,本科,物联网工程师,研究方向:安全研究。
- 姬云豪(2003--),男,汉族,河南安阳市人,本科,网络工程师,研究方向:安全研究。