网络安全分析中的大数据技术应用

（黑龙江职业学院，黑龙江省哈尔滨市，150080）　孙　伟

摘要　本文探讨大数据分析技术在网络安全领域的应用措施，提高安全防护水平和效率。通过数据融合、技术融合和跨平台融合等策略，整合不同来源的安全数据，结合其他网络安全技术，打破信息壁垒，提高安全分析的准确性和全面性。大数据分析技术在网络安全领域的应用，可以提高安全防护的效率和效果，形成协同作战能力，提高整体的安全防护水平。结果表明：大数据分析技术在网络安全领域具有广泛的应用前景，通过构建基于大数据分析技术的网络安全平台，可以进一步提高网络安全防护的能力和水平，为保障网络安全提供有力的支持。

关键词　大数据分析技术；网络安全；数据融合；技术融合；跨平台融合

中图分类号：TN915.08　文献标识码：B

文章编号：1008-0899(2024)04-0017-03

随着信息技术的迅猛发展，网络安全问题日益突显。针对网络攻击和威胁，传统的安全防护手段已经无法满足需求。而大数据分析技术的崛起为网络安全提供了新的解决思路。通过对大量的安全数据进行融合、分析和挖掘，可以更加准确地发现潜在的威胁和攻击行为，及时采取措施进行防范和应对。

1　大数据分析技术应用研究

1.1　数据采集

在网络安全分析中，为了全方位地了解网络状态和识别潜在威胁，需要从多个来源获取数据。防火墙日志记录了网络流量的详细信息，可以帮助分析师追踪可疑行为。入侵检测系统（IDS）警报则提供了对潜在攻击行为的实时警告。网络流量数据可以反映网络的整体运行情况，而系统日志则记录了系统和应用程序的运行状态。这些多样化的数据来源为分析师提供了丰富的信息，有助于提高分析结果的准确性和可靠性。由于原始数据可能来自不同的设备和系统，数据的格式和质量可能存在差异。因此，在进行分析之前，需要对这些数据进行转换和清洗。这包括对缺失值、异常值和错误数据进行处理，以及将不同格式的数据统一转换为适合分析的格式。这个过程可以借助数据清洗工具和算法自动化完成，减少了人工干预和提高了处理效率。

1.2　数据检索

网络安全分析需要处理大量数据，这些数据可能来源于不同的设备和系统，具有多样性和复杂性。分析师需要通过数据检索，快速定位到与网络安全事件或异常行为相关的数据，以便进行深入分析。数据检索可以通过简单的关键字查询、组合查询或高级查询语句实现。同时，一些大数据分析平台也提供了基于机器学习算法的智能化检索功能，可以根据数据特征和分析需求，自动筛选出关键信息。为了提高数据检索的效率和准确性，需要对检索算法进行优化。这包括改进查询语句、优化索引结构、减少数据冗余等。同时，还需要考虑数据的时效性和可扩展性，以满足不同场景下的分析需求[1]。

1.3　数据储存

在数据储存方面，常用的技术包括分布式文件系统（如 Hadoop 的 HDFS）和 NoSQL 数据库（如 MongoDB、Cassandra 等）。这些技术可以处理大量的结构化和非结构化数据，并提供高可靠性和可扩展性的存储解决方案。例如，Hadoop 的 HDFS 可以存储 PB 级别的数据，并且可以将数据分布在多个节点上，提供了高可靠性和容错性。而 NoSQL 数据

作者简介：孙伟（1988~），男，汉族，安徽亳州人，硕士研究生，讲师，研究方向：大数据技术。

课题名称：校企合作产教融合业态中大数据技术专业人才培养研究；课题来源：黑龙江职业学院校级课题；课题编号：XJYB2022079

库则可以处理大量的非结构化数据，提供了高性能和数据一致性保障。

1.4 数据处理

网络安全分析中的大数据技术应用涉及到大量的数据处理需求，因为网络安全分析需要提取出隐藏在大量数据中的有用信息，以便进行威胁检测、异常行为识别等分析工作。因此，数据处理是网络安全分析中大数据技术应用的核心环节之一。在数据处理方面，常用的技术包括数据挖掘、机器学习和深度学习等。这些技术可以从大量的数据中提取出有用的特征和信息，进而进行分类、聚类、异常检测等分析工作。机器学习技术则可以利用训练数据构建模型，对新的数据进行分类或预测，从而实现对未知威胁的检测和识别。深度学习技术则可以处理更为复杂的非线性问题，提高分析的准确性和效率[2]。

2 构建大数据分析应用安全策略

2.1 加强数据保护与安全建设

确保数据在传输和存储过程中的安全性，防止数据被非法获取或篡改。例如，许多金融机构使用SSL/TLS加密技术来保护客户的数据传输，同时采用AES等加密算法对敏感数据进行存储加密。设立严格的数据访问权限和身份验证机制，确保只有授权人员能够访问相关数据。例如，采用多因素身份验证，结合密码策略和权限管理，控制用户对数据的访问。确保在发生安全事故或数据损失时，能迅速恢复数据。定期备份数据，并存储在安全可靠的位置。例如，在医疗大数据分析中，对患者的姓名、身份证号等敏感信息进行脱敏处理。记录所有用户对数据的访问和操作，确保可追溯性，及时发现并应对异常行为[3]。

2.2 提升大数据网络安全感知能力

2.2.1 异常行为检测

通过大数据分析技术，可以实时监测网络流量和用户行为等数据的异常情况，及时发现潜在的攻击行为。通过建立正常行为模型，可以对偏离正常模式的网络流量和用户行为进行报警，有效防范DDoS攻击、数据泄露等安全风险。例如，一些系统利用机器学习算法对网络流量进行分析，学习正常的网络流量模式，当检测到异常流量行为时，会自动触发报警机制，及时通知安全团队进行处理。这种异常行为检测技术可以大大提高网络安全防护的主动性和实时性，减少被攻击的风险。

2.2.2 威胁情报分析

通过收集和分析大量的网络安全情报数据，可以识别出潜在的威胁源和攻击手法，提前预警并采取措施进行防范。黑客论坛、暗网等渠道是获取威胁情报的重要途径。通过分析这些情报数据，可以发现新的漏洞利用方式和攻击手段，及时完善防御措施。例如，一些安全团队利用自然语言处理技术对黑客论坛讨论的内容进行分析，提取出关于漏洞利用和攻击手段的关键信息，为防御提供重要的参考。

2.2.3 关联分析

运用大数据技术，可以将来自不同来源的安全数据进行关联分析，揭示出攻击者的行动模式和意图。通过分析同一时间内多个系统日志的异常事件，可以发现它们之间存在关联性，从而确认这是一次有组织的网络攻击。例如，一些系统利用数据挖掘技术对安全日志进行分析，发现多个异常事件之间的关联性，进而判断出这是一次针对特定目标的攻击行为。这种关联分析技术可以帮助安全团队快速定位攻击源和攻击手法，提高应对效率。

2.2.4 态势感知

通过大数据分析，可以对网络安全态势进行全面感知和评估，提供决策支持。通过可视化技术展示网络安全状况，可以帮助管理者快速了解当前的安全形势，做出合适的应对策略。例如，一些安全管理系统利用数据可视化技术对网络安全数据进行展示，提供直观的网络安全态势感知界面，帮助管理者全面了解网络安全的整体情况，及时做出决策和调整安全策略。这种态势感知技术可以提高网络安全管理的效率和准确性，为企业的网络安全保驾护航。

2.3 提升大数据网络安全融合能力

2.3.1 数据融合

通过大数据技术，可以将来自不同来源、不同格式的安全数据进行融合，形成一个统一的安全数据集。这有助于提高安全分析的准确性和全面性，因为不同来源的数据可以提供不同的视角和信息，综合这些数据可以更全面地了解网络安全状况。例如，网络日志可以提供关于网络流量和行为的信

息，系统监控数据可以提供关于系统运行状态和性能的信息，威胁情报可以提供关于已知威胁和攻击手段的信息。将这些数据进行融合，可以获得更全面的安全视图，帮助安全团队更准确地判断安全形势，做出更合适的应对策略。

2.3.2 技术融合

将大数据分析与其他网络安全技术进行融合，可以形成协同作战的能力，提高安全防护的效率和效果。例如，将大数据分析与入侵检测系统、防火墙等安全设备相结合，可以通过对这些设备产生的数据进行分析，更准确地判断是否存在入侵行为，并及时采取行动进行防范。这种技术融合可以提高安全设备的智能化水平和自动化程度，减少人工干预的需求，提高安全防护的效率和准确性。

2.3.3 跨平台融合

通过大数据技术，可以实现跨平台的安全数据融合和分析，打破不同系统之间的信息壁垒。这有助于提高整体的安全防护水平，因为不同操作系统和应用程序可能存在不同的安全漏洞和风险，将这些数据进行融合分析可以更全面地了解整个系统的安全状况。

2.4 构建基于大数据分析技术的网络安全平台

2.4.1 数据采集和整合

基于大数据分析技术的网络安全平台可以采集来自不同来源的安全数据，包括网络流量数据、系统日志、应用程序数据等。这些数据可以从企业的内部网络和外部网络、不同的操作系统和应用程序、以及各种安全设备中收集。通过数据采集和整合，该平台可以将这些分散的数据整合到一个统一的数据存储系统中，为后续的大数据分析提供丰富的数据基础。

2.4.2 大数据分析

该平台利用先进的大数据分析技术对采集到的数据进行深入分析。这包括异常行为检测，即通过对网络流量、用户行为等数据的实时监测，发现偏离正常模式的行为；威胁情报分析，即通过分析大量的网络安全情报数据，识别出潜在的威胁源和攻击手法；关联分析，即运用大数据技术将来自不同来源的安全数据进行关联分析，揭示出攻击者的行动模式和意图。这些分析可以帮助平台发现潜在的安全风险，并提供决策支持[4]。

2.4.3 实时监控和预警

该平台提供实时的安全监控功能，及时发现异常行为和威胁，并进行预警。通过实时监控，平台可以在第一时间发现网络攻击或异常行为，通过预警机制及时通知安全团队进行处理。提高网络安全防护的主动性和实时性，减少被攻击的风险。

2.4.4 可视化展示

该平台提供可视化的安全数据分析结果展示，帮助管理者快速了解当前的安全形势，做出合适的应对策略。通过数据可视化技术，平台可以将复杂的安全数据分析结果以直观、易懂的方式展示出来，让管理者能够快速了解网络安全状况，从而做出准确的决策和调整安全策略。这可以提高网络安全管理的效率和准确性，为企业的网络安全保驾护航。

3 结语

大数据分析技术在网络安全领域的应用具有重要意义。数据融合、技术融合和跨平台融合等措施可以提高安全分析的准确性和全面性，帮助安全团队更好地识别潜在威胁和攻击行为，以确保网络安全。构建基于大数据分析技术的网络安全平台更是提供了全方位的防护措施，通过数据采集和整合、大数据分析、实时监控和预警以及可视化展示等功能，能够及时发现异常行为、提供实时预警，并为决策者提供直观、易懂的网络安全状态，为网络安全保驾护航。

参考文献

[1]邢敏．互联网金融风险及防范对策的探讨[J]．长春金融高等专科学校学报，2018(4)：57-61．

[2]石松．大数据时代背景下的计算机信息处理方式分析[J]．信息记录材料，2020，21(7)：217-218．

[3]李伟洪．大数据时代计算机网络信息安全与防护措施[J]．电子技术与软件工程，2019(8)：201．

[4]董明．大数据发展对软件个人信息安全的影响[J]．电子技术与软件工程，2019(8)：204．