(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 118200019 B
(45)授权公告日 2024.09.20

(21)申请号 202410443479.X
(22)申请日 2024.04.12
(65)同一申请的已公布的文献号
申请公布号 CN 118200019 A
(43)申请公布日 2024.06.14
(73)专利权人 国网湖北省电力有限公司信息通信公司
地址 430077 湖北省武汉市洪山区徐东大街341号
(72)发明人 卢萍 张勇 冯浩 郭峰 邱爽 焦翰琳 张先飞 张雄 童永飞 张晨燕 周煜廷 黄诚轩 廖荣涛 刘芬 王逸兮 罗弦 叶宇轩 董亮 黄俊东 余铮 冯伟东 代静 袁慧 詹伟
(74)专利代理机构 武汉楚天专利事务所 42113
专利代理师 胡盛登
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 41/16(2022.01)
(56)对比文件
CN 106888196 A,2017.06.23
CN 112671807 A,2021.04.16
审查员 李彦欣

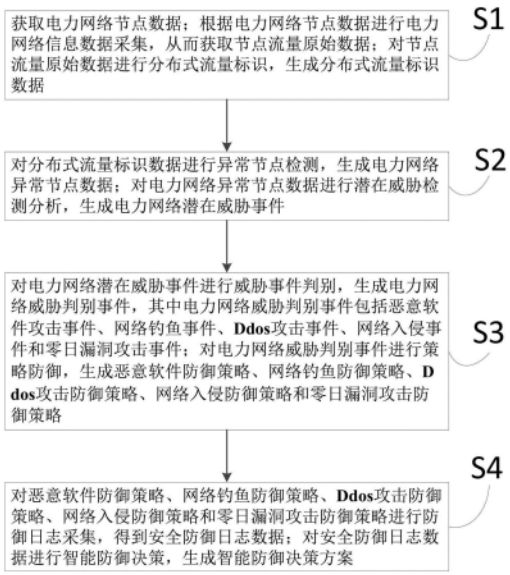
权利要求书4页 说明书18页 附图4页

(54)发明名称

一种网络事件安全监测方法及系统

(57)摘要

本发明涉及数据安全技术领域,尤其涉及一种网络事件安全监测方法及系统。所述方法包括以下步骤:获取电力网络节点数据;根据电力网络节点数据进行电力网络信息数据采集,从而获取节点流量原始数据;对节点流量原始数据进行分布式流量标识,生成分布式流量标识数据;对分布式流量标识数据进行异常节点检测,生成电力网络异常节点数据;对电力网络异常节点数据进行潜在威胁检测分析,生成电力网络潜在威胁事件。本发明通过对网络事件进行异常节点标识以及多层次攻击类型防御策略构建,提高了网络安全防护的全面性和适应性。



CN 118200019 B

1.一种网络事件安全监测方法,其特征在于,包括以下步骤:

步骤S1:获取电力网络节点数据;根据电力网络节点数据进行电力网络信息数据采集,从而获取节点流量原始数据;对节点流量原始数据进行分布式流量标识,将节点流量数据划分为区块或流量片段,并为每个区块或流量片段生成唯一的标识符,生成分布式流量标识数据;

步骤S2:对分布式流量标识数据进行异常节点检测,生成电力网络异常节点数据;对电力网络异常节点数据进行潜在威胁检测分析,生成电力网络潜在威胁事件;

步骤S3:对电力网络潜在威胁事件进行威胁事件判别,生成电力网络威胁判别事件,其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件;对电力网络威胁判别事件进行策略防御,生成恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略;

步骤S4:对恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行防御日志采集,得到安全防御日志数据;对安全防御日志数据进行智能防御决策,生成智能防御决策方案;

步骤S4包括以下步骤:

步骤S41:将恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行策略整合,生成网络事件防御策略;利用网络事件防御策略对电力网络潜在威胁事件进行防御日志采集,得到安全防御日志数据;

步骤S42:对安全防御日志数据进行数据集划分,生成模型训练集和模型测试集;利用决策树模型对模型训练集进行模型训练,生成智能防御决策训练模型;通过模型测试集对智能防御决策训练模型进行模型测试,生成智能防御决策模型;

步骤S43:利用智能防御决策模型对电力网络潜在威胁事件进行智能防御决策,生成智能防御决策方案。

2.根据权利要求1所述的网络事件安全监测方法,其特征在于,步骤S1包括以下步骤:

步骤S11:获取电力网络节点数据;

步骤S12:根据电力网络节点数据进行分布式感知节点部署,得到分布式电力网络感知节点;基于分布式电力网络感知节点进行电力网络信息数据采集,从而获取节点流量原始数据,其中电力网络信息数据采集包括数据包解析、数据包过滤和数据包嗅探;

步骤S13:对节点流量原始数据进行数据预处理,生成标准节点流量原始数据,其中数据预处理包括数据清洗、数据缺失值填充和数据标准化;

步骤S14:对标准节点流量原始数据进行分布式流量标识,生成分布式流量标识数据。

3.根据权利要求2所述的网络事件安全监测方法,其特征在于,步骤S14包括以下步骤:

步骤S141:对标准节点流量原始数据进行网络上传溯源,得到分布式电力流量传输上传节点数据;对分布式电力流量传输上传节点数据进行上传频率分析,得到分布式电力流量传输上传频率数据;

步骤S142:根据分布式电力流量传输上传频率数据对标准节点流量原始数据进行相邻节点最短传输路径计算,得到相邻节点最短路径数据;根据相邻节点最短路径数据对标准节点流量原始数据进行传输闭环通路构建,生成节点传输闭环通路;

步骤S143:基于节点传输闭环通路和分布式电力流量传输上传频率数据进行节点上传

活跃度分析,生成节点上传活跃度分析数据;将节点上传活跃度分析数据和预设的节点上传活跃度阈值进行对比,当节点上传活跃度分析数据大于或等于预设的节点上传活跃度阈值时,则对相应的标准节点流量原始数据进行流量标识,生成分布式流量标识数据。

4.根据权利要求1所述的网络事件安全监测方法,其特征在于,步骤S2包括以下步骤:

步骤S21:对分布式流量标识数据进行异常节点检测,生成电力网络异常节点数据;

步骤S22:根据电力网络异常节点数据进行异常关联关系探索,生成异常关联关系矩阵;

步骤S23:通过电力网络异常节点数据和异常关联关系矩阵进行复杂网络结构建模,生成电力网络复杂网络结构;对电力网络复杂网络结构进行低维向量空间嵌入,生成电力网络异常图谱;

步骤S24:利用电力网络异常图谱对电力网络异常节点数据进行潜在威胁检测分析,生成电力网络潜在威胁事件。

5.根据权利要求4所述的网络事件安全监测方法,其特征在于,步骤S21包括以下步骤:

步骤S211:对分布式流量标识数据进行节点发送接收比率分析,得到节点发送接收比率数据;基于节点发送接收比率对分布式流量标识数据进行数据包大小分析,生成节点发送数据包大小比率数据;

步骤S212:基于节点发送接收比率数据和节点发送数据包大小比率数据对分布式流量标识数据进行网络传输流量速率变化分析,生成节点传输流量速率变化比率数据;

步骤S213:利用节点流量特征比率计算公式对节点发送接收比率数据、节点发送数据包大小比率数据和节点传输流量速率变化比率数据进行节点流量特征比率计算,得到节点流量特征比率数据;

步骤S214:将节点流量特征比率数据和预设的标准节点流量特征比率进行对比,当节点流量特征比率数据大于或等于预设的标准节点流量特征比率时,则生成电力网络异常节点数据。

6.根据权利要求5所述的网络事件安全监测方法,其特征在于,步骤S213中的节点流量特征比率计算公式如下所示:

$$R(t')=\int_0^t\left[\frac{F_s(t')}{\sqrt{1+\left(\frac{D_s(t')}{D_{\max}}\right)^2}}\cdot\frac{P_s(t')}{P_{\max}}-\frac{F_r(t')}{\sqrt{1+\left(\frac{D_r(t')}{D_{\max}}\right)^2}}\cdot\frac{P_r(t')}{P_{\max}}\right]dt';$$

式中,$R(t')$表示为节点在时间t'的流量特征比率,$F_s(t')$表示为节点在时间t'的发送数据包大小占其最大发送数据包大小的比率,$D_s(t')$表示为节点在时间t'的发送数据包传输流量速率变化占其最大传输流量速率的比率,$D_{\max}$表示为节点的最大传输流量速率,$P_s(t')$表示为节点在时间t'的发送接收比率,$P_{\max}$表示为节点的最大发送接收比率,$F_r(t')$表示为节点在时间t'的接收数据包大小占其最大接收数据包大小的比率,

$D_r(t')$表示为节点在时间t'的接收数据包传输流量速率变化占其最大传输流量速率的比率，t表示为节点检测时间上限，$P_r(t')$表示为节点在时间t'的接收数据包发送接收比率，t'表示为时间点。

7.根据权利要求4所述的网络事件安全监测方法，其特征在于，步骤S24包括以下步骤：

步骤S241：利用电力网络异常图谱对电力网络异常节点数据进行威胁行为关联图构建，生成网络威胁行为图谱；对网络威胁行为图谱进行节点中心性分析，生成网络节点中心性指标，其中网络节点中心性指标包括节点度中心性、节点介数中心性和节点接近中心性；

步骤S242：根据节点度中心性、节点介数中心性和节点接近中心性对电力网络异常图谱进行威胁行为社区划分，生成网络威胁行为社区标识数据；基于网络威胁行为社区标识数据对电力网络异常节点数据进行相似行为聚类，生成异常节点行为聚类数据；

步骤S243：对异常节点行为聚类数据进行威胁路径识别，生成威胁行为路径识别数据；对威胁行为路径识别数据进行威胁行为强关联分析，生成威胁行为关键路径识别数据；

步骤S244：根据威胁行为关键路径识别数据对电力网络异常节点数据进行潜在威胁关联分析，生成电力网络潜在威胁事件。

8.根据权利要求1所述的网络事件安全监测方法，其特征在于，步骤S3包括以下步骤：

步骤S31：对电力网络潜在威胁事件进行威胁事件判别，生成电力网络威胁判别事件，其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件；

步骤S32：确认电力网络威胁判别事件为恶意软件攻击事件时，则对电力网络异常节点数据进行节点防火墙部署，得到异常节点防火墙；基于异常节点防火墙进行入侵检测以及入侵防御，得到网络流量数据和异常节点行为数据；根据网络流量数据和异常节点行为数据对电力网络异常节点进行最小网络控制权限调整，生成恶意软件防御策略；

步骤S33：确认电力网络威胁判别事件为网络钓鱼事件时，则对电力网络异常节点数据进行电子邮件过滤器设置，得到邮件过滤器配置规则数据；基于邮件过滤器配置规则数据对电力网络异常节点数据进行数据上传多因素认证强制，生成网络钓鱼防御策略；

步骤S34：确认电力网络威胁判别事件为Ddos攻击事件时，则对电力网络异常节点数据进行攻击时段分析，生成攻击密集时段数据；根据攻击密集时段数据对电力网络异常节点进行负载均衡，生成负载均衡数据；对负载均衡数据和预设的标准负载均衡阈值进行判别，当负载均衡数据大于预设的标准负载均衡阈值时，则对超出部分的电力网络异常节点数据进行路由黑洞，生成Ddos攻击防御策略；

步骤S35：确认电力网络威胁判别事件为网络入侵事件时，则对电力网络异常节点数据进行入侵区域分析，得到入侵区域分析数据；基于入侵区域分析数据进行网络隔离，生成网络隔离区域数据；利用网络隔离区域数据对入侵区域进行安全修复，生成网络入侵防御策略；

步骤S36：确认电力网络威胁判别事件为零日漏洞攻击事件时，则对电力网络异常节点数据进行威胁情报分析，生成威胁情报分析数据；对威胁情报分析数据进行零日漏洞补丁应用，生成零日漏洞补丁数据；根据零日漏洞补丁数据对电力网络异常节点进行流量规则

过滤,生成零日漏洞攻击防御策略。

9.一种网络事件安全监测系统,其特征在于,用于执行如权利要求1所述的网络事件安全监测方法,该网络事件安全监测系统包括:

分布式标识模块,用于获取电力网络节点数据;根据电力网络节点数据进行电力网络信息数据采集,从而获取节点流量原始数据;对节点流量原始数据进行分布式流量标识,生成分布式流量标识数据;

潜在威胁分析模块,用于对分布式流量标识数据进行异常节点检测,生成电力网络异常节点数据;对电力网络异常节点数据进行潜在威胁检测分析,生成电力网络潜在威胁事件;

策略防御模块,用于对电力网络潜在威胁事件进行威胁事件判别,生成电力网络威胁判别事件,其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件;对电力网络威胁判别事件进行策略防御,生成恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略;

智能决策模块,用于对恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行防御日志采集,得到安全防御日志数据;对安全防御日志数据进行智能防御决策,生成智能防御决策方案。

一种网络事件安全监测方法及系统

技术领域

[0001] 本发明涉及数据安全技术领域,尤其涉及一种网络事件安全监测方法及系统。

背景技术

[0002] 随着电力系统的扩张,高压输电线路和发电厂的建设成为发展的重点。这一阶段安全检测方法开始涉及电力系统的稳定性和短路保护,以确保系统在异常情况下能够稳定运行。随着数据挖掘和人工智能技术的不断发展,电力系统安全检测迈入新阶段。基于数据驱动的方法逐渐成为主流,包括使用机器学习和深度学习技术。这些方法可以从大量的实时数据中识别模式和异常,提高了检测的准确性和效率。物联网技术的应用使得电力系统能够更好地实现设备之间的互联互通。边缘计算技术的发展使得数据处理更加迅速和有效。安全检测方法逐渐向实时、分布式方向发展,能够在系统各个节点上进行事件检测和响应。然而目前传统方法在异常节点检测和威胁分析上往往使用静态规则或基于历史数据的方法,容易受限于固定的规则和模式,无法有效应对新型威胁,同时对于威胁事件判别和策略防御上常常缺乏全面性和及时性,导致网络的整体防护能力不足。

发明内容

[0003] 基于此,有必要提供一种网络事件安全监测方法及系统,以解决至少一个上述技术问题。

[0004] 为实现上述目的,一种网络事件安全监测方法,所述方法包括以下步骤:

[0005] 步骤S1:获取电力网络节点数据;根据电力网络节点数据进行电力网络信息数据采集,从而获取节点流量原始数据;对节点流量原始数据进行分布式流量标识,生成分布式流量标识数据;

[0006] 步骤S2:对分布式流量标识数据进行异常节点检测,生成电力网络异常节点数据;对电力网络异常节点数据进行潜在威胁检测分析,生成电力网络潜在威胁事件;

[0007] 步骤S3:对电力网络潜在威胁事件进行威胁事件判别,生成电力网络威胁判别事件,其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件;对电力网络威胁判别事件进行策略防御,生成恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略;

[0008] 步骤S4:对恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行防御日志采集,得到安全防御日志数据;对安全防御日志数据进行智能防御决策,生成智能防御决策方案。

[0009] 本发明通过获取节点流量原始数据并进行分布式流量标识,可以实现对电力网络的实时监测和检测,有助于及时发现异常节点和潜在威胁事件,提高网络的安全性。在步骤S2中对分布式流量标识数据进行异常节点检测,可以有效识别出电力网络中的异常行为节点,有助于及时发现存在的攻击或异常情况。根据异常节点数据进行潜在威胁检测分析,能

够识别出电力网络潜在的威胁事件,有助于提前预警网络安全威胁,为进一步的防御做好准备。对潜在威胁事件进行判别,并生成相应的电力网络威胁判别事件,例如恶意软件攻击、网络钓鱼、DDoS攻击、网络入侵和零日漏洞攻击等。同时,根据这些事件生成相应的防御策略,有针对性地应对各类安全威胁。对安全防御日志数据进行智能防御决策,可以基于实时数据和历史数据,通过机器学习或人工智能技术生成智能防御决策方案,有助于自动化和优化安全防御流程,提高网络安全的响应速度和效率。通过生成恶意软件防御策略、网络钓鱼防御策略、DDoS攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略,形成了多层次的安全防御体系,多维度的防御能力能够有效降低网络受到各类威胁的风险。对防御策略进行防御日志采集,有助于记录安全事件和响应过程,为后续的安全审计和改进提供数据支持。因此,本发明通过对网络事件进行异常节点标识以及多层次攻击类型防御策略构建,提高了网络安全防护的全面性和适应性。

[0010] 在本说明书中,提供了一种网络事件安全检测系统,用于执行上述的网络事件安全检测方法,该网络事件安全检测系统包括:

[0011] 分布式标识模块,用于获取电力网络节点数据;根据电力网络节点数据进行电力网络信息数据采集,从而获取节点流量原始数据;对节点流量原始数据进行分布式流量标识,生成分布式流量标识数据;

[0012] 潜在威胁分析模块,用于对分布式流量标识数据进行异常节点检测,生成电力网络异常节点数据;对电力网络异常节点数据进行潜在威胁检测分析,生成电力网络潜在威胁事件;

[0013] 策略防御模块,用于对电力网络潜在威胁事件进行威胁事件判别,生成电力网络威胁判别事件,其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件;对电力网络威胁判别事件进行策略防御,生成恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略;

[0014] 智能决策模块,用于对恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行防御日志采集,得到安全防御日志数据;对安全防御日志数据进行智能防御决策,生成智能防御决策方案。

[0015] 本发明的有益效果在于通过对分布式流量标识数据进行异常节点检测和潜在威胁分析,可以发现电力网络中存在的异常节点和潜在威胁事件,有助于及早发现潜在的攻击或异常情况,提高网络安全的监控和响应能力。针对电力网络潜在威胁事件,进行威胁事件判别并生成相应的威胁判别事件,有助于对不同类型的威胁进行分类和识别,从而能够采取特定的防御策略和措施,如恶意软件防御策略、网络钓鱼防御策略、DDoS攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略。通过防御日志采集和智能防御决策,可以利用安全防御日志数据进行智能化的防御决策,有助于根据实时的安全日志和网络状态,自动生成具有针对性和智能化的防御方案,以及应对威胁事件的决策建议。因此,本发明通过对网络事件进行异常节点标识以及多层次攻击类型防御策略构建,提高了网络安全防护的全面性和适应性。

附图说明

[0016] 图1为一种网络事件安全监测方法的步骤流程示意图；

[0017] 图2为图1中步骤S2的详细实施步骤流程示意图；

[0018] 图3为图2中步骤S24的详细实施步骤流程示意图；

[0019] 图4为图1中步骤S3的详细实施步骤流程示意图；

[0020] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0021] 下面结合附图对本发明专利的技术方法进行清楚、完整的描述，显然，所描述的实施例是本发明的一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域所属的技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0022] 此外，附图仅为本发明的示意性图解，并非一定是按比例绘制。图中相同的附图标记表示相同或类似的部分，因而将省略对它们的重复描述。附图中所示的一些方框图是功能实体，不一定必须与物理或逻辑上独立的实体相对应。可以采用软件形式来实现功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器方法和/或微控制器方法中实现这些功能实体。

[0023] 应当理解的是，虽然在这里可能使用了术语“第一”、“第二”等等来描述各个单元，但是这些单元不应当受这些术语限制。使用这些术语仅仅是为了将一个单元与另一个单元进行区分。举例来说，在不背离示例性实施例的范围的情况下，第一单元可以被称为第二单元，并且类似地第二单元可以被称为第一单元。这里所使用的术语“和/或”包括其中一个或更多所列出的相关联项目的任意和所有组合。

[0024] 为实现上述目的，请参阅图1至图4，一种网络事件安全监测方法，所述方法包括以下步骤：

[0025] 步骤S1：获取电力网络节点数据；根据电力网络节点数据进行电力网络信息数据采集，从而获取节点流量原始数据；对节点流量原始数据进行分布式流量标识，生成分布式流量标识数据；

[0026] 步骤S2：对分布式流量标识数据进行异常节点检测，生成电力网络异常节点数据；对电力网络异常节点数据进行潜在威胁检测分析，生成电力网络潜在威胁事件；

[0027] 步骤S3：对电力网络潜在威胁事件进行威胁事件判别，生成电力网络威胁判别事件，其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件；对电力网络威胁判别事件进行策略防御，生成恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略；

[0028] 步骤S4：对恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行防御日志采集，得到安全防御日志数据；对安全防御日志数据进行智能防御决策，生成智能防御决策方案。

[0029] 本发明通过获取节点流量原始数据并进行分布式流量标识，可以实现对电力网络的实时监测和检测，有助于及时发现异常节点和潜在威胁事件，提高网络的安全性。在步骤

S2中对分布式流量标识数据进行异常节点检测,可以有效识别出电力网络中的异常行为节点,有助于及时发现存在的攻击或异常情况。根据异常节点数据进行潜在威胁检测分析,能够识别出电力网络潜在的威胁事件,有助于提前预警网络安全威胁,为进一步的防御做好准备。对潜在威胁事件进行判别,并生成相应的电力网络威胁判别事件,例如恶意软件攻击、网络钓鱼、DDoS攻击、网络入侵和零日漏洞攻击等。同时,根据这些事件生成相应的防御策略,有针对性地应对各类安全威胁。对安全防御日志数据进行智能防御决策,可以基于实时数据和历史数据,通过机器学习或人工智能技术生成智能防御决策方案,有助于自动化和优化安全防御流程,提高网络安全的响应速度和效率。通过生成恶意软件防御策略、网络钓鱼防御策略、DDoS攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略,形成了多层次的安全防御体系,多维度的防御能力能够有效降低网络受到各类威胁的风险。对防御策略进行防御日志采集,有助于记录安全事件和响应过程,为后续的安全审计和改进提供数据支持。因此,本发明通过对网络事件进行异常节点标识以及多层次攻击类型防御策略构建,提高了网络安全防护的全面性和适应性。

[0030] 本发明实施例中,参考图1所述,为本发明一种网络事件安全监测方法的步骤流程示意图,在本实例中,所述一种网络事件安全监测方法包括以下步骤:

[0031] 步骤S1:获取电力网络节点数据;根据电力网络节点数据进行电力网络信息数据采集,从而获取节点流量原始数据;对节点流量原始数据进行分布式流量标识,生成分布式流量标识数据;

[0032] 本发明实施例中,通过确定电力网络的拓扑结构,包括各个节点的位置、连接关系等。收集电力网络设备和传感器的信息,如变电站、配电站、电力线路等。获取电力网络的实时监测数据,如电流、电压、功率等。部署数据采集设备或传感器来收集电力网络的实时数据。配置和管理数据采集设备,确保其能够准确和稳定地采集到节点的数据。使用传统的通信协议(如Modbus、DNP3等)或现代化的通信技术(如物联网、通信卫星等)进行数据采集。利用分布式流量标识技术,将节点流量数据进行标记和识别,以便后续的异常检测和分析。使用合适的算法和方法,将节点流量数据划分为合理的区块或流量片段,并为每个区块或流量片段生成唯一的标识符。确保分布式流量标识的准确性和有效性,以便后续的异常检测和安全分析能够基于标识数据进行。

[0033] 步骤S2:对分布式流量标识数据进行异常节点检测,生成电力网络异常节点数据;对电力网络异常节点数据进行潜在威胁检测分析,生成电力网络潜在威胁事件;

[0034] 本发明实施例中,通过使用合适的异常检测算法,如基于统计方法、机器学习方法或深度学习方法等,来检测电力网络中的异常节点。基于分布式流量标识数据,对每个节点的流量特征进行分析,以识别与正常行为不符的异常节点。设置适当的阈值或规则,用于判断哪些节点被标识为异常节点。对异常节点数据进行库分析,与已知的威胁库或攻击模式进行比对,以确定潜在的威胁类型。利用威胁情报和安全专家的知识,进行行为分析和模式识别,以发现未知或新兴的潜在威胁。进行网络拓扑分析,找出异常节点与其他节点之间的关联,以确定潜在的威胁传播路径。基于检测到的异常节点和潜在威胁分析的结果,将相关的异常节点和威胁类型整合,生成电力网络的潜在威胁事件。对潜在威胁事件进行综合评估,包括评估威胁的严重程度、影响范围和紧急性,以确定响应和防御措施。

[0035] 步骤S3:对电力网络潜在威胁事件进行威胁事件判别,生成电力网络威胁判别事

件,其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件;对电力网络威胁判别事件进行策略防御,生成恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略;

[0036] 本发明实施例中,通过基于潜在威胁事件的特征和行为模式,使用机器学习、行为分析或规则引擎等方法来进行威胁事件判别。通过使用Yara规则库,用于识别恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件等。结合实时监测和日志分析,对电力网络的流量、行为和事件进行实时验证和判断。将判别的威胁事件与步骤S2中生成的电力网络潜在威胁事件进行匹配和更新,以确保准确的威胁事件判别。针对不同的威胁判别事件,制定相应的防御策略,包括恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略。针对恶意软件攻击事件,实施安全防护措施,如使用杀毒软件、防火墙、反恶意软件工具等来检测、隔离和清除恶意软件。针对网络钓鱼事件,加强网络安全意识培训,使用反钓鱼技术和防钓鱼策略来识别和阻止钓鱼攻击。针对Ddos攻击事件,实施流量清洗、流量限制、入侵检测和负载均衡等防御措施,以减轻攻击的影响。针对网络入侵事件,部署入侵检测系统(IDS)和入侵防御系统(IPS),及时检测和阻止入侵行为,并及时更新安全补丁来修复漏洞。针对零日漏洞攻击事件,建立紧急响应团队,及时跟踪和应对新发现的漏洞,并实施补丁管理和漏洞修复工作。

[0037] 步骤S4:对恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行防御日志采集,得到安全防御日志数据;对安全防御日志数据进行智能防御决策,生成智能防御决策方案。

[0038] 本发明实施例中,通过配置安全设备和系统,使其能够产生相应的防御日志数据,具体为防火墙、入侵检测系统(IDS)、入侵防御系统(IPS)、安全信息和事件管理系统(SIEM)等。确保设备和系统的日志功能已启用,并配置适当的日志级别和日志格式。设置日志采集服务器或中央日志管理系统,用于集中收集、存储和管理防御日志数据。针对采集到的安全防御日志数据,使用安全分析和决策支持技术进行智能分析和决策。通过使用Snort、Suricata等IDS系统以及恶意软件特征库,用于检测和分析恶意软件行为、网络钓鱼攻击、Ddos攻击、网络入侵和零日漏洞攻击等。基于分析结果,进行智能防御决策生成,包括自动化响应、警报生成、隔离恶意行为、封锁攻击源IP或协调人工干预等措施。结合业务需求和安全风险评估,制定合适的智能防御策略和决策方案,以提供有效的安全保护和响应。

[0039] 优选的,步骤S1包括以下步骤:

[0040] 步骤S11:获取电力网络节点数据;

[0041] 步骤S12:根据电力网络节点数据进行分布式感知节点部署,得到分布式电力网络感知节点;基于分布式电力网络感知节点进行电力网络信息数据采集,从而获取节点流量原始数据,其中电力网络信息数据采集包括数据包解析、数据包过滤和数据包嗅探;

[0042] 步骤S13:对节点流量原始数据进行数据预处理,生成标准节点流量原始数据,其中数据预处理包括数据清洗、数据缺失值填充和数据标准化;

[0043] 步骤S14:对标准节点流量原始数据进行分布式流量标识,生成分布式流量标识数据。

[0044] 本发明通过在电力网络中部署分布式感知节点,可以实现对多个节点的数据采集

与监测,可以提高电力网络的感知能力和数据覆盖范围。通过分布式电力网络感知节点进行信息数据采集,可以获取节点流量原始数据,原始数据包括了电力网络的实时信息,对于电力系统的监测和分析具有重要意义。对节点流量原始数据进行数据预处理,包括数据清洗、缺失值填充和数据标准化等步骤,预处理操作有助于提高数据的质量和准确性,为后续的分析和处理提供可靠的数据基础。对标准节点流量原始数据进行分布式流量标识,生成分布式流量标识数据,标识可以用于识别和跟踪电力网络中的流量特征,为网络性能分析、异常检测和故障诊断提供支持。

[0045] 本发明实施例中,通过收集电力网络的拓扑结构和节点信息,例如变电站、发电厂、输电线路和配电设备等。获取节点的实时状态数据,如电流、电压、功率等。根据电力网络节点数据,确定分布式感知节点的部署位置,考虑覆盖范围和数据采集需求。部署感知节点并确保其连接到电力网络,确保数据的可靠采集。感知节点通过数据包解析、数据包过滤和数据包嗅探等技术,从电力网络中抓取并采集节点流量原始数据。进行数据清洗,包括去除异常值、噪声数据和重复数据等,确保数据的准确性和一致性。处理数据缺失值,可以采用插值方法填充策略,填充缺失的数据项。进行数据标准化,将节点流量数据转化为符合一定规范和范围的标准数据格式,便于后续的分析和处理。基于标准节点流量原始数据,采用Bloom Filter数据结构进行分布式流量标识的生成。分布式流量标识可包括流量特征、流量行为和流量属性等信息,用于对节点流量进行识别、分类和分析。

[0046] 优选的,步骤S14包括以下步骤:

[0047] 步骤S141:对标准节点流量原始数据进行网络上传溯源,得到分布式电力流量传输上传节点数据;对分布式电力流量传输上传节点数据进行上传频率分析,得到分布式电力流量传输上传频率数据;

[0048] 步骤S142:根据分布式电力流量上传频率数据对标准节点流量原始数据进行相邻节点最短传输路径计算,得到相邻节点最短路径数据;根据相邻节点最短路径数据对标准节点流量原始数据进行传输闭环通路构建,生成节点传输闭环通路;

[0049] 步骤S143:基于节点传输闭环通路和分布式电力流量传输上传频率数据进行节点上传活跃度分析,生成节点上传活跃度分析数据;将节点上传活跃度分析数据和预设的节点上传活跃度阈值进行对比,当节点上传活跃度分析数据大于或等于预设的节点上传活跃度阈值时,则对相应的标准节点流量原始数据进行流量标识,生成分布式流量标识数据。

[0050] 本发明通过对标准节点流量原始数据进行网络上传溯源,可以追踪电力流量的传输路径,有助于了解电力网络中的数据流动,发现潜在的传输问题或异常情况。对分布式电力流量传输上传节点数据进行上传频率分析,可以获取节点数据上传的频率信息。通过分析上传频率数据,可以了解节点的活跃度和数据传输模式,有助于监测节点的数据采集和传输状态。根据分布式电力流量上传频率数据,可以计算节点间的相邻节点最短传输路径。通过寻找最短传输路径,可以优化数据的传输效率,减少能耗和网络延迟。基于相邻节点最短路径数据,可以构建节点传输闭环通路。传输闭环通路的建立可以提高数据传输的可靠性和安全性,防止数据漏洞和传输异常的发生。基于节点传输闭环通路和分布式电力流量传输上传频率数据,进行节点上传活跃度的分析,可以帮助了解节点的上传行为和活跃程度,识别出主要的流量传输节点,用于后续的数据处理和分析。将节点上传活跃度分析数据与预设的节点上传活跃度阈值进行对比,当节点上传活跃度分析数据达到或超过阈值时,

对相应的标准节点流量原始数据进行流量标识,可以用于标记重要的节点和流量数据,为后续的分析、监测和控制提供基础。

[0051] 本发明实施例中,通过收集标准节点流量原始数据,并对其进行网络上传溯源分析。该分析可以使用网络监控工具或技术来确定数据流量的来源和路径。通过网络上传溯源分析,得到分布式电力流量传输上传节点数据。对分布式电力流量传输上传节点数据进行上传频率分析。可以使用统计方法或数据挖掘技术来分析节点数据上传的频率和模式,得到分布式电力流量传输上传频率数据。使用分布式电力流量上传频率数据,对标准节点流量原始数据进行相邻节点最短传输路径计算,可以使用图论算法,如最短路径算法,来找到节点之间的最短传输路径。根据相邻节点最短路径数据,对标准节点流量原始数据进行传输闭环通路构建,可以通过确定节点之间的闭环路径来建立传输闭环通路,以确保数据在网络中的循环传输。基于节点传输闭环通路和分布式电力流量传输上传频率数据,进行节点上传活跃度分析。可以使用统计分析方法来计算节点上传活跃度,并生成节点上传活跃度分析数据。对节点上传活跃度分析数据和预设的节点上传活跃度阈值进行对比。如果节点上传活跃度分析数据大于或等于预设的节点上传活跃度阈值,则对相应的标准节点流量原始数据进行流量标识。生成分布式流量标识数据,以标识高活跃度的节点和相应的流量数据。

[0052] 优选的,步骤S2包括以下步骤:

[0053] 步骤S21:对分布式流量标识数据进行异常节点检测,生成电力网络异常节点数据;

[0054] 步骤S22:根据电力网络异常节点数据进行异常关联关系探索,生成异常关联关系矩阵;

[0055] 步骤S23:通过电力网络异常节点数据和异常关联关系矩阵进行复杂网络结构建模,生成电力网络复杂网络结构;对电力网络复杂网络结构进行低维向量空间嵌入,生成电力网络异常图谱;

[0056] 步骤S24:利用电力网络异常图谱对电力网络异常节点数据进行潜在威胁检测分析,生成电力网络潜在威胁事件。

[0057] 本发明通过对分布式流量标识数据进行异常节点检测,可以有效地识别电力网络中存在异常或异常行为的节点,有助于及早发现并应对网络中的故障、攻击或其他异常情况,防止潜在的网络威胁。根据电力网络异常节点数据,可以通过分析节点之间的异常关联关系,建立异常关联关系矩阵,可以帮助了解电力网络中各节点之间的相互作用和依赖关系,进一步揭示潜在的异常或风险传播路径。通过使用电力网络异常节点数据和异常关联关系矩阵,可以构建电力网络的复杂网络结构,有助于更好地理解电力网络的整体结构和性质,识别出网络中的重要节点和关键路径,为网络管理和风险评估提供支持。对电力网络复杂网络结构进行低维向量空间嵌入,可以将网络中的节点映射到低维空间中,保留节点之间的关系和相似性。通过生成电力网络的异常图谱,可以更直观地展示网络中的异常节点、异常关联和威胁事件,帮助分析人员理解网络状态和威胁情况。利用电力网络异常图谱,可以对电力网络异常节点数据进行潜在威胁检测分析。通过识别网络中的潜在威胁事件,可以帮助网络管理者采取相应的措施来减轻风险、加强网络安全防护,并保障电力系统的正常运行。

[0058] 作为本发明的一个实例,参考图2所示,在本实例中所述步骤S2包括:

[0059] 步骤S21:对分布式流量标识数据进行异常节点检测,生成电力网络异常节点数据;

[0060] 本发明实施例中,通过获取电力网络中的流量标识数据,数据包括电力设备的状态、功率、电压、电流等信息,数据可以通过传感器、监测设备或者智能电表等获取。对获取的数据进行预处理,包括数据清洗、去除噪声、缺失值处理等,有助于提高数据的质量和准确性。从预处理后的数据中提取有用的特征。特征具体为电力设备的各种指标,如功率因数、频率、谐波等。选择合适的特征可以提高异常节点检测的效果。选择适合电力网络的异常节点检测算法。常用的算法包括基于统计的方法(如均值、标准差)、基于机器学习的方法(如支持向量机、随机森林)以及基于深度学习的方法(如自编码器、深度神经网络)等。使用选定的异常节点检测算法对数据进行分析和处理,标识出电力网络中的异常节点。异常节点具体为存在故障的设备、电流、电压异常等。将得到的异常节点标识与原始数据进行匹配,生成电力网络异常节点数据,数据包括异常节点的位置、时间戳、异常类型等。

[0061] 步骤S22:根据电力网络异常节点数据进行异常关联关系探索,生成异常关联关系矩阵;

[0062] 本发明实施例中,通过将步骤S21中生成的电力网络异常节点数据进行整理和准备。确保数据包含有关异常节点的信息,例如节点标识、异常类型、时间戳等。明确异常关联关系的定义。根据电力网络的特点和需求,定义异常节点之间的关联关系。关联关系可以是空间上的关联(如设备之间的物理连接)、时间上的关联(如同时发生的异常事件)、功能上的关联(如相邻设备之间的相互影响关系)等。确定用于衡量异常关联关系强度的指标,具体是统计指标,如相关系数、互信息等,以及基于机器学习或图论的指标,如图结构相似性、节点距离等。选择适当的指标可以量化异常关联关系的强度和相关性。选择相关性分析、聚类分析、关联规则挖掘等算法,算法可以帮助发现异常节点之间的关联模式和规律。根据异常关联关系的探索结果,构建异常关联关系矩阵。矩阵的行和列代表电力网络中的异常节点,矩阵的元素表示节点之间的关联强度。矩阵可以是二维矩阵或者稀疏矩阵,根据网络规模和计算需求进行选择。对生成的异常关联关系矩阵进行分析和解读。通过矩阵的可视化、统计分析和图论分析等方法,可以获取异常节点之间的关联模式、集群结构、异常传播路径等信息。

[0063] 步骤S23:通过电力网络异常节点数据和异常关联关系矩阵进行复杂网络结构建模,生成电力网络复杂网络结构;对电力网络复杂网络结构进行低维向量空间嵌入,生成电力网络异常图谱;

[0064] 本发明实施例中,通过根据电力网络的特点,将异常节点作为网络中的节点,每个节点代表一个异常事件或异常设备。利用异常关联关系矩阵中的关联强度信息,将节点之间的关联关系转化为网络中的边。可以根据关联强度的阈值设置一定的连接条件,仅保留关联强度大于阈值的边。根据实际需求,可以为网络中的节点和边定义一些属性,例如节点类型、边的权重等。对生成的电力网络复杂网络结构进行统计分析。可以计算网络的节点度分布、聚类系数、平均路径长度等指标,了解网络的拓扑特性和结构特征。利用社区发现算法,识别复杂网络中的社区结构。社区结构表示节点之间具有较高的内部连接强度,而节点之间的连接强度较低,可以帮助发现电力网络中的功能模块和异常传播路径。根据复杂网

络结构,提取节点和边的特征。可以利用图论中的方法,如节点中心性、局部和全局特征等,来衡量节点和边在网络中的重要程度和相互关系。应用降维技术,例如主成分分析(PCA)或t-SNE,将高维特征映射到低维空间,可以减少数据的维度,并保留数据的关键结构信息。利用嵌入后的低维特征,将电力网络的异常节点和关联关系可视化为图谱。节点可以用不同的形状、颜色、大小表示,以反映节点的异常类型或属性。边的粗细和颜色可以表示关联强度。对生成的电力网络异常图谱进行分析和解读。通过观察图谱中节点的分布、集群结构、异常传播路径等,可以获取电力网络异常行为的整体情况和局部细节。

[0065] 步骤S24:利用电力网络异常图谱对电力网络异常节点数据进行潜在威胁检测分析,生成电力网络潜在威胁事件。

[0066] 本发明实施例中,通过根据电力网络异常图谱中节点的位置和连接关系,识别具有异常特征的节点,节点是关键设备或系统中的异常节点。通过分析其在图谱中的位置和邻近节点的相互关系,可以评估其潜在的威胁程度。利用异常节点在低维向量空间中的特征向量,结合机器学习或深度学习方法,对异常节点进行分类和检测。可以使用监督学习算法,如支持向量机(SVM)或神经网络,训练模型来区分正常节点和异常节点。根据电力网络异常图谱中的边和连接关系,提取异常节点之间的关联路径,可以通过图论中的遍历算法,如深度优先搜索(DFS)或广度优先搜索(BFS),来获取异常节点之间的最短路径或路径特征。根据异常关联关系的强度,如边的权重或关联程度,对异常关联关系进行评估。可以设置阈值或使用统计方法,如聚类系数或相关系数,来衡量异常关联关系的重要程度。结合异常节点的特征和异常关联关系的分析结果,对电力网络进行威胁评估,具体为根据异常节点的重要性、关联关系的强度和关联路径的特征,评估潜在威胁事件的严重程度和潜在影响,并将评估结果转化为电力网络的潜在威胁事件,对潜在威胁事件进行分类、标记和描述,从而形成系统化的威胁事件库。事件库包括事件的起因、影响范围、后果以及建议的应对措施。

[0067] 优选的,步骤S21包括以下步骤:

[0068] 步骤S211:对分布式流量标识数据进行节点发送接收比率分析,得到节点发送接收比率数据;基于节点发送接收比率对分布式流量标识数据进行数据包大小分析,生成节点发送数据包大小比率数据;

[0069] 步骤S212:基于节点发送接收比率数据和节点发送数据包大小比率数据对分布式流量标识数据进行网络传输流量速率变化分析,生成节点传输流量速率变化比率数据;

[0070] 步骤S213:利用节点流量特征比率计算公式对节点发送接收比率数据、节点发送数据包大小比率数据和节点传输流量速率变化比率数据进行节点流量特征比率计算,得到节点流量特征比率数据;

[0071] 步骤S214:将节点流量特征比率数据和预设的标准节点流量特征比率进行对比,当节点流量特征比率数据大于或等于预设的标准节点流量特征比率时,则生成电力网络异常节点数据。

[0072] 本发明通过对分布式流量标识数据进行节点发送接收比率分析,可以得到节点发送接收比率数据,可以帮助了解每个节点在电力网络中的数据发送和接收情况,识别出发送和接收比率异常的节点。通过基于节点发送接收比率对分布式流量标识数据进行数据包大小分析,可以进一步分析节点的数据包大小情况,有助于识别出数据包大小异常的节点。

利用节点发送接收比率数据和节点发送数据包大小比率数据对分布式流量标识数据进行网络传输流量速率变化分析,可以帮助监测节点的传输流量速率变化情况,检测出流量速率异常的节点。通过分析传输流量速率的变化,可以及时发现异常情况,防止潜在的网络问题进一步扩大。利用节点流量特征比率计算公式对节点发送接收比率数据、节点发送数据包大小比率数据和节点传输流量速率变化比率数据进行节点流量特征比率计算,可以综合考虑节点在多个方面的流量特征,生成节点流量特征比率数据。通过计算节点的流量特征比率,可以更全面地评估节点的流量特征,发现潜在的异常。将节点流量特征比率数据与预设的标准节点流量特征比率进行对比,当节点流量特征比率数据大于或等于预设的标准节点流量特征比率时,会生成电力网络异常节点数据,可以自动化地识别出异常节点,减少了人工的主观判断,提高了异常节点的检测效率。通过及时发现和标识异常节点,可以采取相应的修复措施,防止异常节点对电力网络造成进一步的损害。

[0073] 本发明实施例中,通过收集分布式流量标识数据,包括节点的发送和接收数据量。使用适当的算法和工具对节点的发送接收比率进行分析,计算每个节点的发送接收比率数据。利用节点的发送接收比率数据,对分布式流量标识数据进行数据包大小分析,生成节点的发送数据包大小比率数据。基于节点的发送接收比率数据和发送数据包大小比率数据,对分布式流量标识数据进行网络传输流量速率变化分析。使用适当的算法和工具来计算节点的传输流量速率变化比率数据。根据预先定义的节点流量特征比率计算公式,结合节点的发送接收比率数据、发送数据包大小比率数据和传输流量速率变化比率数据,进行节点流量特征比率计算。确定计算公式中的权重和参数,以便准确地评估节点的流量特征。将节点流量特征比率数据与预设的标准节点流量特征比率进行对比。如果节点流量特征比率数据大于或等于预设的标准节点流量特征比率,则认为该节点是电力网络的异常节点。生成电力网络异常节点数据,可以保存在数据库中或以其他方式进行记录和处理。

[0074] 优选的,步骤S213中的节点流量特征比率计算公式具体如下:

[0075] $$R(t')=\int_0^t\left[\frac{F_s(t')}{\sqrt{1+\left(\frac{D_s(t')}{D_{\max}}\right)^2}}\cdot\frac{P_s(t')}{P_{\max}}-\frac{F_r(t')}{\sqrt{1+\left(\frac{D_r(t')}{D_{\max}}\right)^2}}\cdot\frac{P_r(t')}{P_{\max}}\right]dt';$$

[0076] 式中,$R(t')$表示为节点在时间t'的流量特征比率,$F_s(t')$表示为节点在时间t'的发送数据包大小占其最大发送数据包大小的比率,$D_s(t')$表示为节点在时间t'的发送数据包传输流量速率变化占其最大传输流量速率的比率,D_{max}表示为节点的最大传输流量速率,$P_s(t')$表示为节点在时间t'的发送接收比率,P_{max}表示为节点的最大发送接收比率,$F_r(t')$表示为节点在时间t'的接收数据包大小占其最大接收数据包大小的比率,$D_r(t')$表示为节点在时间t'的接收数据包传输流量速率变化占其最大传输流量速率的比率,t表示为节点检测时间上限,$P_r(t')$表示为节点在时间t'的接收数据包发送接收比率,t'表示为时间点。

[0077] 本发明通过分析并整合了一种节点流量特征比率计算公式,公式中的$\frac{F_s(t')}{\sqrt{1+\left(\frac{D_s(t')}{D_{\max}}\right)^2}}$描述了节点发送数据包大小比率$F_s(t')$和发送数据包传输流量速率变化比率$D_s(t')$对节点

流量特征比率的影响。通过发送接收比率$P_s(t')$权衡,确保节点的发送数据包大小比率和传输流量速率变化比率都得到适当的考虑。除法操作用于归一化传输流量速率变化比率,使其与发送数据包大小比率在计算上具有相同的权重。$\frac{F_r(t')}{\sqrt{1+\left(\frac{D_r(t')}{D_{max}}\right)^2}}$描述了节点接收数据包大小比率$F_r(t')$和接收数据包传输流量速率变化比率$D_r(t')$对节点流量特征比率的影响。通过接收数据包发送接收比率$P_r(t')$权衡,确保节点的接收数据包大小比率和传输流量速率变化比率都得到适当的考虑。同样,除法操作用于归一化传输流量速率变化比率。时间的积分,表示了在时间范围内这两个项对节点流量特征比率的累积影响。公式考虑了节点在一段时间内的各种输入和状态变化对流量特征比率的综合影响,更贴近实际网络中节点的动态变化。在使用本领域常规的节点流量特征比率计算公式时,可以得到节点在时间t′的流量特征比率,通过应用本发明提供的节点流量特征比率计算公式,可以更加精确的计算出节点在时间t′的流量特征比率。公式综合考虑了节点的发送和接收数据包大小比率、传输流量速率变化比率以及发送接收比率的特征,从而提供了节点流量特征比率的综合评估。通过使用发送接收比率来权衡发送和接收数据包大小比率以及传输流量速率变化比率,确保每个因素在计算中得到了适当的考虑。通过除以各自的最大值,将传输流量速率变化比率归一化,使其在计算中具有相同的权重,避免了某一方面因素对结果产生过大的影响。通过时间积分,考虑了节点在一段时间内的状态变化,使得结果更加贴近实际网络中节点流量特征比率的变化趋势。

[0078] 优选的,步骤S24包括以下步骤:

[0079] 步骤S241:利用电力网络异常图谱对电力网络异常节点数据进行威胁行为关联图构建,生成网络威胁行为图谱;对网络威胁行为图谱进行节点中心性分析,生成网络节点中心性指标,其中网络节点中心性指标包括节点度中心性、节点介数中心性和节点接近中心性;

[0080] 步骤S242:根据节点度中心性、节点介数中心性和节点接近中心性对电力网络异常图谱进行威胁行为社区划分,生成网络威胁行为社区标识数据;基于网络威胁行为社区标识数据对电力网络异常节点数据进行相似行为聚类,生成异常节点行为聚类数据;

[0081] 步骤S243:对异常节点行为聚类数据进行威胁路径识别,生成威胁行为路径识别数据;对威胁行为路径识别数据进行威胁行为强关联分析,生成威胁行为关键路径识别数据;

[0082] 步骤S244:根据威胁行为关键路径识别数据对电力网络异常节点数据进行潜在威胁关联分析,生成电力网络潜在威胁事件。

[0083] 本发明通过构建威胁行为关联图和网络节点中心性分析,可以生成网络威胁行为图谱,有助于可视化和理解电力网络中的威胁行为,从而提高对异常节点的识别和分析能力。根据节点度中心性、节点介数中心性和节点接近中心性等指标,将电力网络异常图谱划分为威胁行为社区。然后,对每个社区内的异常节点进行相似行为聚类,可以更好地理解和分析不同节点集群的威胁行为,帮助发现隐藏的威胁模式和趋势。对异常节点行为聚类数据进行威胁路径识别,可以识别出潜在的威胁行为路径。随后,进行威胁行为强关联分析,找到关键路径,即具有重要影响力和高风险的威胁行为路径,有助于集中精力应对关键威

胁,提高网络安全的响应效率和准确性。利用威胁行为关键路径识别数据,对电力网络异常节点数据进行潜在威胁关联分析,有助于发现异常节点之间存在的隐藏威胁关系,对潜在的威胁事件进行早期预警和预防。

[0084] 作为本发明的一个实例,参考图3所示,在本实例中所述步骤S24包括:

[0085] 步骤S241:利用电力网络异常图谱对电力网络异常节点数据进行威胁行为关联图构建,生成网络威胁行为图谱;对网络威胁行为图谱进行节点中心性分析,生成网络节点中心性指标,其中网络节点中心性指标包括节点度中心性、节点介数中心性和节点接近中心性;

[0086] 本发明实施例中,通过收集电力网络异常节点数据,可以通过监测设备、传感器或日志数据获取。然后,根据异常节点之间的关联关系,构建电力网络异常图谱。可以使用图论和网络分析的技术和算法,如图数据库或图分析工具,来表示和处理异常图谱。利用电力网络异常图谱,将异常节点之间的威胁行为关联关系加入到图谱中,可以通过将威胁行为表示为图的边(或连接)来完成。威胁行为包括恶意访问、攻击、数据篡改等。在图谱中,异常节点表示为图的节点,而威胁行为表示为节点之间的边。对生成的网络威胁行为图谱进行节点中心性分析,计算节点的中心性指标。常用的节点中心性指标包括:节点度中心性:度中心性是指节点在图中与其他节点相连的数量。具有较高度中心性的节点在网络中具有更多的连接,具有更多的影响力和关键性。节点介数中心性:介数中心性是指节点在网络中作为最短路径上的桥梁的次数。具有高介数中心性的节点在信息传播和影响传递方面起着重要的作用。节点接近中心性:接近中心性是指节点与其他节点之间的平均最短路径距离。具有较高接近中心性的节点更容易访问其他节点,在网络中具有更大的控制能力。

[0087] 步骤S242:根据节点度中心性、节点介数中心性和节点接近中心性对电力网络异常图谱进行威胁行为社区划分,生成网络威胁行为社区标识数据;基于网络威胁行为社区标识数据对电力网络异常节点数据进行相似行为聚类,生成异常节点行为聚类数据;

[0088] 本发明实施例中,通过计算节点度中心性、节点介数中心性和节点接近中心性指标。根据之前生成的网络威胁行为图谱,使用合适的算法计算每个节点的度中心性、介数中心性和接近中心性。结合这些中心性指标,可以使用社区发现算法,如Louvain算法、谱聚类算法等,对电力网络异常图谱进行社区划分,算法能够将具有相似中心性特征的节点聚集到同一个社区中,从而形成威胁行为社区。在社区划分完成后,为每个社区分配一个唯一的标识,生成网络威胁行为社区标识数据,标识可以用于标识和区分不同的威胁行为社区。使用网络威胁行为社区标识数据来对电力网络异常节点数据进行聚类。将每个异常节点与其所属的威胁行为社区关联。选择适当的聚类算法,如K均值聚类、层次聚类、密度聚类等,根据异常节点的特征和相似性进行聚类。根据聚类结果,生成异常节点行为聚类数据。每个聚类包含具有相似行为特征的异常节点。

[0089] 步骤S243:对异常节点行为聚类数据进行威胁路径识别,生成威胁行为路径识别数据;对威胁行为路径识别数据进行威胁行为强关联分析,生成威胁行为关键路径识别数据;

[0090] 本发明实施例中,通过针对每个异常节点行为聚类,分析其中的行为序列或事件序列。使用合适的算法,如序列模式挖掘算法(如Apriori算法、GSP算法)、马尔可夫模型等,对异常节点行为聚类中的行为序列进行挖掘,以识别潜在的威胁行为路径。根据识别到的

威胁行为路径,生成威胁行为路径识别数据,数据包含路径的起点、终点、中间经过的节点或行为,以及路径的频率或概率信息。使用威胁行为路径识别数据作为输入,采用关联规则挖掘算法,如Apriori算法、FP-Growth算法等,进行威胁行为强关联分析。对挖掘得到的关联规则,可以使用支持度和置信度等指标进行评估和筛选,选择具有较高关联性的规则。根据关联规则的评估结果,生成威胁行为关键路径识别数据,数据包含关键路径或关联规则的信息,如起点、终点、关联规则的条件与结果等。

[0091] 步骤S244:根据威胁行为关键路径识别数据对电力网络异常节点数据进行潜在威胁关联分析,生成电力网络潜在威胁事件。

[0092] 本发明实施例中,通过收集电力网络异常节点数据,包括节点行为日志、事件记录等,数据记录了电力网络中的异常行为或事件。获取威胁行为关键路径识别数据,包括关键路径的起点、终点和关联规则等信息。根据威胁行为关键路径识别数据中的关键路径信息,将电力网络异常节点数据与关键路径进行匹配。对于匹配成功的异常节点数据,分析其与关键路径的关联性,并计算相应的关联度指标,如支持度、置信度等。基于关联度指标,筛选出具有较高关联度的异常节点数据,作为潜在威胁事件候选集。对潜在威胁事件候选集进行进一步的分析和筛选,考虑事件的属性、时序、频率等信息,排除误报或冗余事件。根据分析结果,生成电力网络潜在威胁事件列表,包括事件的描述、关联的异常节点或行为信息、事件发生的时间窗口等。

[0093] 优选的,步骤S3包括以下步骤:

[0094] 步骤S31:对电力网络潜在威胁事件进行威胁事件判别,生成电力网络威胁判别事件,其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件;

[0095] 步骤S32:确认电力网络威胁判别事件为恶意软件攻击事件时,则对电力网络异常节点数据进行节点防火墙部署,得到异常节点防火墙;基于异常节点防火墙进行入侵检测以及入侵防御,得到网络流量数据和异常节点行为数据;根据网络流量数据和异常节点行为数据对电力网络异常节点进行最小网络控制权限调整,生成恶意软件防御策略;

[0096] 步骤S33:确认电力网络威胁判别事件为网络钓鱼事件时,则对电力网络异常节点数据进行电子邮件过滤器设置,得到邮件过滤器配置规则数据;基于邮件过滤器配置规则数据对电力网络异常节点数据进行数据上传多因素认证强制,生成网络钓鱼防御策略;

[0097] 步骤S34:确认电力网络威胁判别事件为Ddos攻击事件时,则对电力网络异常节点数据进行攻击时段分析,生成攻击密集时段数据;根据攻击密集时段数据对电力网络异常节点进行负载均衡,生成负载均衡数据;对负载均衡数据和预设的标准负载均衡阈值进行判别,当负载均衡数据大于预设的标准负载均衡阈值时,则对超出部分的电力网络异常节点数据进行路由黑洞,生成Ddos攻击防御策略;

[0098] 步骤S35:确认电力网络威胁判别事件为网络入侵事件时,则对电力网络异常节点数据进行入侵区域分析,得到入侵区域分析数据;基于入侵区域分析数据进行网络隔离,生成网络隔离区域数据;利用网络隔离区域数据对入侵区域进行安全修复,生成网络入侵防御策略;

[0099] 步骤S36:确认电力网络威胁判别事件为零日漏洞攻击事件时,则对电力网络异常节点数据进行威胁情报分析,生成威胁情报分析数据;对威胁情报分析数据进行零日漏洞

补丁应用,生成零日漏洞补丁数据;根据零日漏洞补丁数据对电力网络异常节点进行流量规则过滤,生成零日漏洞攻击防御策略。

[0100] 本发明通过对电力网络潜在威胁事件进行威胁事件判别可以识别出不同类型的威胁事件,包括恶意软件攻击、网络钓鱼、Ddos攻击、网络入侵和零日漏洞攻击,有助于精确识别对电力网络安全造成威胁的事件。对于确认为恶意软件攻击事件的情况,部署异常节点防火墙并进行入侵检测和入侵防御,可以提高对恶意软件的防护能力。最小网络控制权限调整可以限制异常节点的网络访问权限,增强对恶意软件的防御策略。确定为网络钓鱼事件时,设置电子邮件过滤器和数据上传多因素认证强制,有助于防止电力网络中的网络钓鱼行为,防御策略可以有效减少恶意邮件的传递和遏制社交工程攻击。确认为Ddos攻击事件时,进行攻击时段分析和负载均衡可以平衡网络负载,减轻网络的压力。通过判别超过标准负载均衡阈值的部分节点并进行路由黑洞,可以有效防止Ddos攻击对电力网络的影响。确定为网络入侵事件时,进行入侵区域分析和网络隔离,有助于识别入侵区域并将其与其他网络隔离,遏制入侵的扩散。随后的安全修复措施可以修复入侵区域的漏洞,增强电力网络的防御能力。确认为零日漏洞攻击事件时,进行威胁情报分析和零日漏洞补丁应用,有助于监测和处理新出现的安全威胁。通过流量规则过滤,可以有效阻止利用零日漏洞的攻击,提高系统的安全性。

[0101] 作为本发明的一个实例,参考图4所示,在本实例中所述步骤S3包括:

[0102] 步骤S31:对电力网络潜在威胁事件进行威胁事件判别,生成电力网络威胁判别事件,其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件;

[0103] 本发明实施例中,通过收集电力网络的各项数据,包括网络流量、设备日志、安全事件日志等。通过分析这些数据,可以发现任何异常活动、异常流量模式或异常事件,并将它们标识为潜在的威胁事件。与威胁情报和漏洞数据库进行数据对比和匹配,以了解已知的威胁事件和漏洞攻击。通过将收集到的数据与已知的模式进行对比,可以快速识别出恶意软件攻击、网络钓鱼、Ddos攻击、网络入侵和零日漏洞攻击事件。利用机器学习和人工智能技术,构建模型和算法,对收集到的数据进行分析和处理,可以自动学习和识别出电力网络中的异常行为模式,并将其与已知的威胁模式进行比较,从而准确判断潜在的威胁事件。通过监测系统的异常节点、异常流量和异常行为,可以及时发现和识别恶意软件攻击、网络钓鱼、Ddos攻击、网络入侵和零日漏洞攻击事件。使用各种技术,如入侵检测系统(IDS)和行为分析系统(BAS),可以对电力网络中的节点和流量进行实时监测和检测。电力网络安全专家可以通过审查和分析数据,提供专业的意见和判断。他们可以根据自身的经验和知识对潜在的威胁事件进行评估,确定其是否为恶意软件攻击、网络钓鱼、Ddos攻击、网络入侵或零日漏洞攻击事件。

[0104] 步骤S32:确认电力网络威胁判别事件为恶意软件攻击事件时,则对电力网络异常节点数据进行节点防火墙部署,得到异常节点防火墙;基于异常节点防火墙进行入侵检测以及入侵防御,得到网络流量数据和异常节点行为数据;根据网络流量数据和异常节点行为数据对电力网络异常节点进行最小网络控制权限调整,生成恶意软件防御策略;

[0105] 本发明实施例中,通过根据已确认的异常节点,在电力网络中针对这些节点进行防火墙的部署,防火墙可以监控和过滤与该节点相关的网络流量,以阻止潜在的恶意软件

攻击。防火墙的配置需要根据电力网络的特定需求进行调整。通过异常节点防火墙对电力网络进行入侵检测和入侵防御。入侵检测系统可以分析网络流量数据和异常节点行为数据,以便及时发现存在的恶意软件攻击行为。入侵防御措施包括及时响应和阻止入侵行为,以保护电力网络的安全性。利用网络流量数据和异常节点行为数据进行分析,以了解攻击者的行为模式和攻击方式。通过流量分析,可以确定恶意软件攻击的特征和目标,从而制定有效的防御策略。根据网络流量数据和异常节点行为数据,对电力网络异常节点进行最小网络控制权限的调整,包括对异常节点进行审计和限制其网络访问权限,以减轻安全风险。基于分析结果和最小网络控制权限调整,生成恶意软件防御策略,策略包括对恶意软件攻击行为的检测规则、阻止规则和响应措施等。

[0106] 步骤S33:确认电力网络威胁判别事件为网络钓鱼事件时,则对电力网络异常节点数据进行电子邮件过滤器设置,得到邮件过滤器配置规则数据;基于邮件过滤器配置规则数据对电力网络异常节点数据进行数据上传多因素认证强制,生成网络钓鱼防御策略;

[0107] 本发明实施例中,通过确定合适的电子邮件过滤器软件或服务来过滤电力网络中收发的电子邮件。配置过滤器以识别和拦截潜在的网络钓鱼邮件,包括设置规则、黑名单、白名单、关键字过滤等。根据电力网络的需求和安全政策,调整过滤器的灵敏度和策略。在配置邮件过滤器时,记录所使用的规则和设置,以便后续参考和审查,记录包括过滤器版本、规则列表、策略配置等信息。确认采用多因素认证技术来增强电力网络中异常节点的登录安全性。配置多因素认证,例如使用密码、令牌、生物识别等多个身份验证因素进行登录验证。强制所有电力网络异常节点使用多因素认证,并严格限制只有通过多因素认证才能访问关键系统和数据。基于邮件过滤器配置规则数据和数据上传多因素认证强制,生成网络钓鱼防御策略,策略包括配置合适的过滤规则、完善的多因素认证设置和相应的安全策略指南。

[0108] 步骤S34:确认电力网络威胁判别事件为Ddos攻击事件时,则对电力网络异常节点数据进行攻击时段分析,生成攻击密集时段数据;根据攻击密集时段数据对电力网络异常节点进行负载均衡,生成负载均衡数据;对负载均衡数据和预设的标准负载均衡阈值进行判别,当负载均衡数据大于预设的标准负载均衡阈值时,则对超出部分的电力网络异常节点数据进行路由黑洞,生成Ddos攻击防御策略;

[0109] 本发明实施例中,通过对电力网络异常节点数据进行分析,确定Ddos攻击发生的时间段,可以通过监测网络流量、识别异常数据包以及分析攻击模式来实现。攻击时段分析的目的是确定哪些时间段受到攻击最为密集,以便后续的负载均衡措施。根据攻击时段分析的结果,生成攻击密集时段数据,数据可以标识出攻击活动高发的时间段,为后续的负载均衡提供依据。根据攻击密集时段数据,对电力网络的异常节点进行负载均衡调整。负载均衡的目的是均衡网络负载,以减轻受攻击节点的负担,确保网络的正常运行。根据进行负载均衡调整后的结果,生成负载均衡数据,数据描述了每个节点的负载状态,包括当前负载水平、处理能力等信息。将负载均衡数据与预设的标准负载均衡阈值进行比较。如果某个节点的负载均衡数据超过了设定的阈值,即负载过大,表示该节点正受到攻击并超出了正常负载范围。对超出负载均衡阈值的部分电力网络异常节点数据采取路由黑洞措施。路由黑洞是一种措施,将异常节点的流量引导到一个无效地址或丢弃该流量,从而有效阻止攻击流量进入网络。根据路由黑洞的实施结果,生成Ddos攻击防御策略。该策略包括针对Ddos攻击

的具体防御措施,如黑洞路由配置、流量过滤、攻击流量标识等,以保护电力网络免受Ddos攻击的影响。

[0110] 步骤S35:确认电力网络威胁判别事件为网络入侵事件时,则对电力网络异常节点数据进行入侵区域分析,得到入侵区域分析数据;基于入侵区域分析数据进行网络隔离,生成网络隔离区域数据;利用网络隔离区域数据对入侵区域进行安全修复,生成网络入侵防御策略;

[0111] 本发明实施例中,通过对电力网络异常节点数据进行入侵区域分析,包括识别入侵节点、分析入侵路径、确定入侵节点之间的关系等。入侵区域分析的目的是确定受到入侵的具体区域和节点,为后续的网络隔离提供依据。根据入侵区域分析的结果,生成入侵区域分析数据,数据描述了入侵事件发生的区域和相关节点的信息,包括入侵节点的位置、攻击方式等。基于入侵区域分析数据,进行网络隔离操作。网络隔离可以将受到入侵的区域或节点与其他部分隔离开来,以防止入侵事件的扩散和影响其它部分的电力网络。根据进行网络隔离的结果,生成网络隔离区域数据,数据描述了已经隔离的区域或节点的信息,包括隔离的方式、隔离范围等。利用网络隔离区域数据,对入侵区域进行安全修复。安全修复包括修复已受到入侵的系统、补丁安装、提升安全配置等措施,以恢复受影响区域的正常状态。根据安全修复的结果,生成网络入侵防御策略。该策略包括针对网络入侵的具体防御措施,如入侵检测系统的部署、访问控制策略的优化、加强认证和授权等,以增强电力网络的安全性。

[0112] 步骤S36:确认电力网络威胁判别事件为零日漏洞攻击事件时,则对电力网络异常节点数据进行威胁情报分析,生成威胁情报分析数据;对威胁情报分析数据进行零日漏洞补丁应用,生成零日漏洞补丁数据;根据零日漏洞补丁数据对电力网络异常节点进行流量规则过滤,生成零日漏洞攻击防御策略。

[0113] 本发明实施例中,通过对电力网络异常节点数据进行威胁情报分析,包括对攻击事件的特征、来源、方法等进行分析,以获取关于零日漏洞攻击的情报信息。通过分析威胁情报,可以了解攻击者的策略、目的以及攻击方式。根据威胁情报分析的结果,生成威胁情报分析数据,数据包括关键信息,例如已知的零日漏洞攻击的特征、攻击指令、漏洞的影响范围等。针对已知的零日漏洞攻击,根据威胁情报分析数据进行相应的补丁应用,包括下载和安装针对漏洞的修复补丁,更新软件版本,或者进行相关配置调整。根据零日漏洞补丁应用的结果,生成零日漏洞补丁数据,数据描述了已应用的补丁信息,包括补丁的版本、应用时间等。根据零日漏洞补丁数据,对电力网络异常节点进行流量规则过滤,涉及配置防火墙、入侵检测系统等网络设备,以筛选和过滤通过网络节点的流量,阻止包含零日漏洞攻击的恶意流量进入受影响的节点。根据流量规则过滤的结果,生成零日漏洞攻击的防御策略。该策略包括特定的阻断规则、应用层过滤规则、流量监控策略等,以减轻零日漏洞攻击的风险,保护电力网络的安全。

[0114] 优选的,步骤S4包括以下步骤:

[0115] 步骤S41:将恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行策略整合,生成网络事件防御策略;利用网络事件防御策略对电力网络潜在威胁事件进行防御日志采集,得到安全防御日志数据;

[0116] 步骤S42:对安全防御日志数据进行数据集划分,生成模型训练集和模型测试集;

利用决策树模型对模型训练集进行模型训练,生成智能防御决策训练模型;通过模型测试集对智能防御决策训练模型进行模型测试,生成智能防御决策模型;

[0117] 步骤S43:利用智能防御决策模型对电力网络潜在威胁事件进行智能防御决策,生成智能防御决策方案。

[0118] 本发明通过将恶意软件防御策略、网络钓鱼防御策略、DDoS攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行整合,可以有效提高电力网络的整体安全性,确保多个安全方面的综合防护。利用智能防御决策模型,可以实现对电力网络潜在威胁事件的智能分析和决策,帮助网络安全人员更快速、准确地响应威胁,提供针对性的防御措施,降低漏报漏检的风险,并加强对新型威胁和未知威胁的应对能力。通过对安全防御日志数据的分析和模型训练,可以发现潜在的安全威胁和攻击模式,并生成智能防御决策方案,从而在发生安全事件时能够更及时、有效地采取防御措施,提高电力网络的安全防护能力。

[0119] 本发明实施例中,通过将恶意软件防御策略、网络钓鱼防御策略、DDoS攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行整合,生成网络事件防御策略,包括指定特定的配置规则、设置防御参数、部署安全设备等。接着,利用网络事件防御策略对电力网络潜在威胁事件进行防御日志采集,以获取安全防御日志数据。对安全防御日志数据进行数据集划分,生成模型训练集和模型测试集,可以通过按照一定比例划分数据集,确保训练集和测试集的样本分布的代表性。然后,使用决策树模型对模型训练集进行模型训练。决策树模型是一种有监督学习方法,能够根据输入的特征对样本进行分类和预测。利用训练好的决策树模型对电力网络潜在威胁事件进行智能防御决策。通过使用安全防御日志数据和相关特征作为输入,决策树模型可以自动进行分析和判断,确定威胁事件的等级、类型和应对策略,能够生成智能防御决策方案,提供具体的防御措施和行动建议。

[0120] 在本说明书中,提供了一种网络事件安全检测系统,用于执行上述的网络事件安全检测方法,该网络事件安全检测系统包括:

[0121] 分布式标识模块,用于获取电力网络节点数据;根据电力网络节点数据进行电力网络信息数据采集,从而获取节点流量原始数据;对节点流量原始数据进行分布式流量标识,生成分布式流量标识数据;

[0122] 潜在威胁分析模块,用于对分布式流量标识数据进行异常节点检测,生成电力网络异常节点数据;对电力网络异常节点数据进行潜在威胁检测分析,生成电力网络潜在威胁事件;

[0123] 策略防御模块,用于对电力网络潜在威胁事件进行威胁事件判别,生成电力网络威胁判别事件,其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件;对电力网络威胁判别事件进行策略防御,生成恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略;

[0124] 智能决策模块,用于对恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行防御日志采集,得到安全防御日志数据;对安全防御日志数据进行智能防御决策,生成智能防御决策方案。

[0125] 本发明的有益效果在于通过对分布式流量标识数据进行异常节点检测和潜在威胁分析,可以发现电力网络中存在的异常节点和潜在威胁事件,有助于及早发现潜在的攻

击或异常情况,提高网络安全的监控和响应能力。针对电力网络潜在威胁事件,进行威胁事件判别并生成相应的威胁判别事件,有助于对不同类型的威胁进行分类和识别,从而能够采取特定的防御策略和措施,如恶意软件防御策略、网络钓鱼防御策略、DDoS攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略。通过防御日志采集和智能防御决策,可以利用安全防御日志数据进行智能化的防御决策,有助于根据实时的安全日志和网络状态,自动生成具有针对性和智能化的防御方案,以及应对威胁事件的决策建议。因此,本发明通过对网络事件进行异常节点标识以及多层次攻击类型防御策略构建,提高了网络安全防护的全面性和适应性。

[0126] 因此,无论从哪一点来看,均应将实施例看作是示范性的,而且是非限制性的,本发明的范围由所附权利要求而不是上述说明限定,因此旨在将落在申请文件的等同要件的含义和范围内的所有变化涵括在本发明内。

[0127] 以上所述仅是本发明的具体实施方式,使本领域技术人员能够理解或实现本发明。对这些实施例的多种修改对本领域的技术人员来说将是显而易见的,本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下,在其它实施例中实现。因此,本发明将不会被限制于本文所示的这些实施例,而是要符合与本文所发明的原理和新颖特点相一致的最宽的范围。

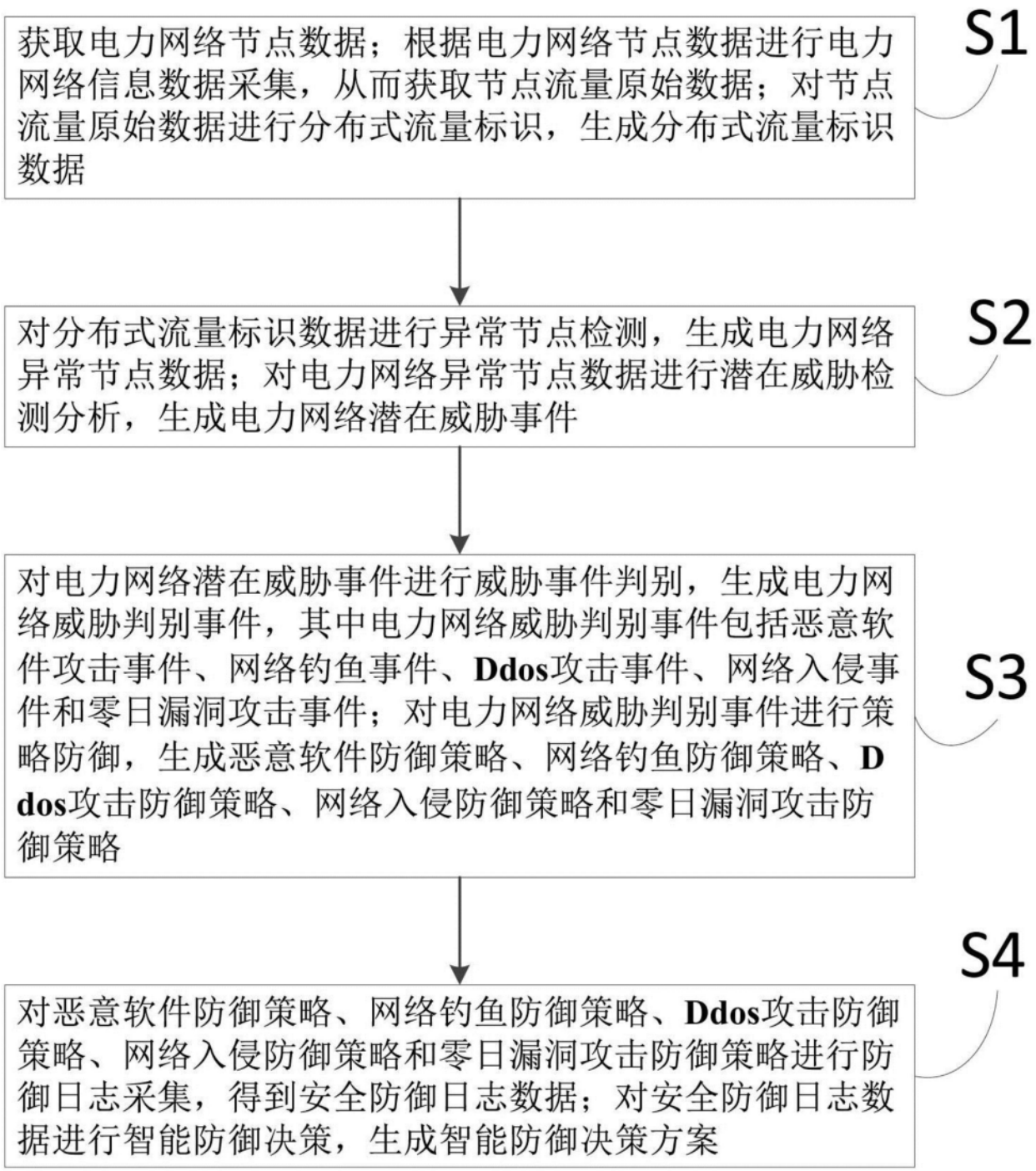

S1
获取电力网络节点数据；根据电力网络节点数据进行电力网络信息数据采集，从而获取节点流量原始数据；对节点流量原始数据进行分布式流量标识，生成分布式流量标识数据
S2
对分布式流量标识数据进行异常节点检测，生成电力网络异常节点数据；对电力网络异常节点数据进行潜在威胁检测分析，生成电力网络潜在威胁事件
S3
对电力网络潜在威胁事件进行威胁事件判别，生成电力网络威胁判别事件，其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件；对电力网络威胁判别事件进行策略防御，生成恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略
S4
对恶意软件防御策略、网络钓鱼防御策略、Ddos攻击防御策略、网络入侵防御策略和零日漏洞攻击防御策略进行防御日志采集，得到安全防御日志数据；对安全防御日志数据进行智能防御决策，生成智能防御决策方案

图1

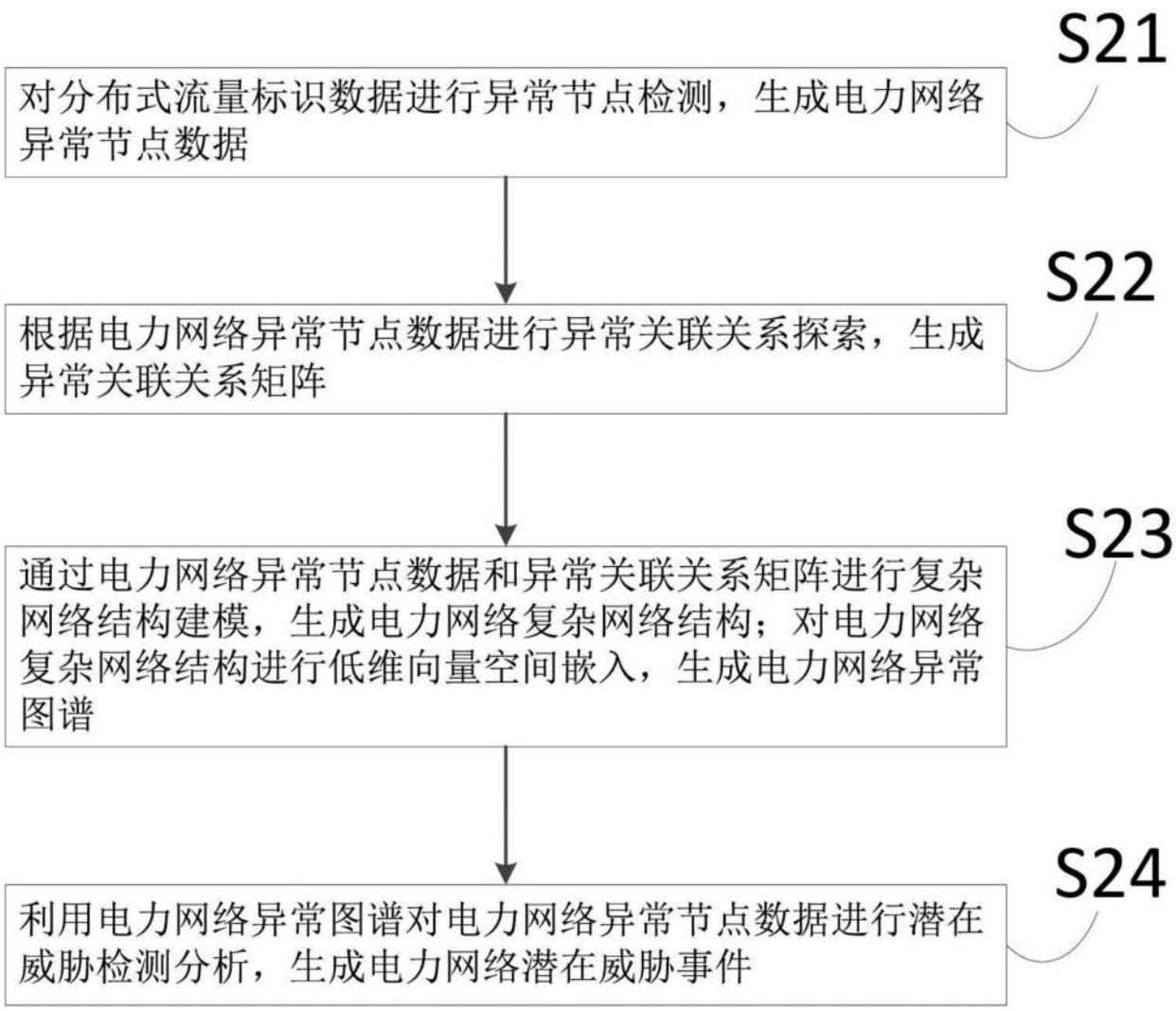

S21
对分布式流量标识数据进行异常节点检测，生成电力网络异常节点数据
S22
根据电力网络异常节点数据进行异常关联关系探索，生成异常关联关系矩阵
S23
通过电力网络异常节点数据和异常关联关系矩阵进行复杂网络结构建模，生成电力网络复杂网络结构；对电力网络复杂网络结构进行低维向量空间嵌入，生成电力网络异常图谱
S24
利用电力网络异常图谱对电力网络异常节点数据进行潜在威胁检测分析，生成电力网络潜在威胁事件

图2

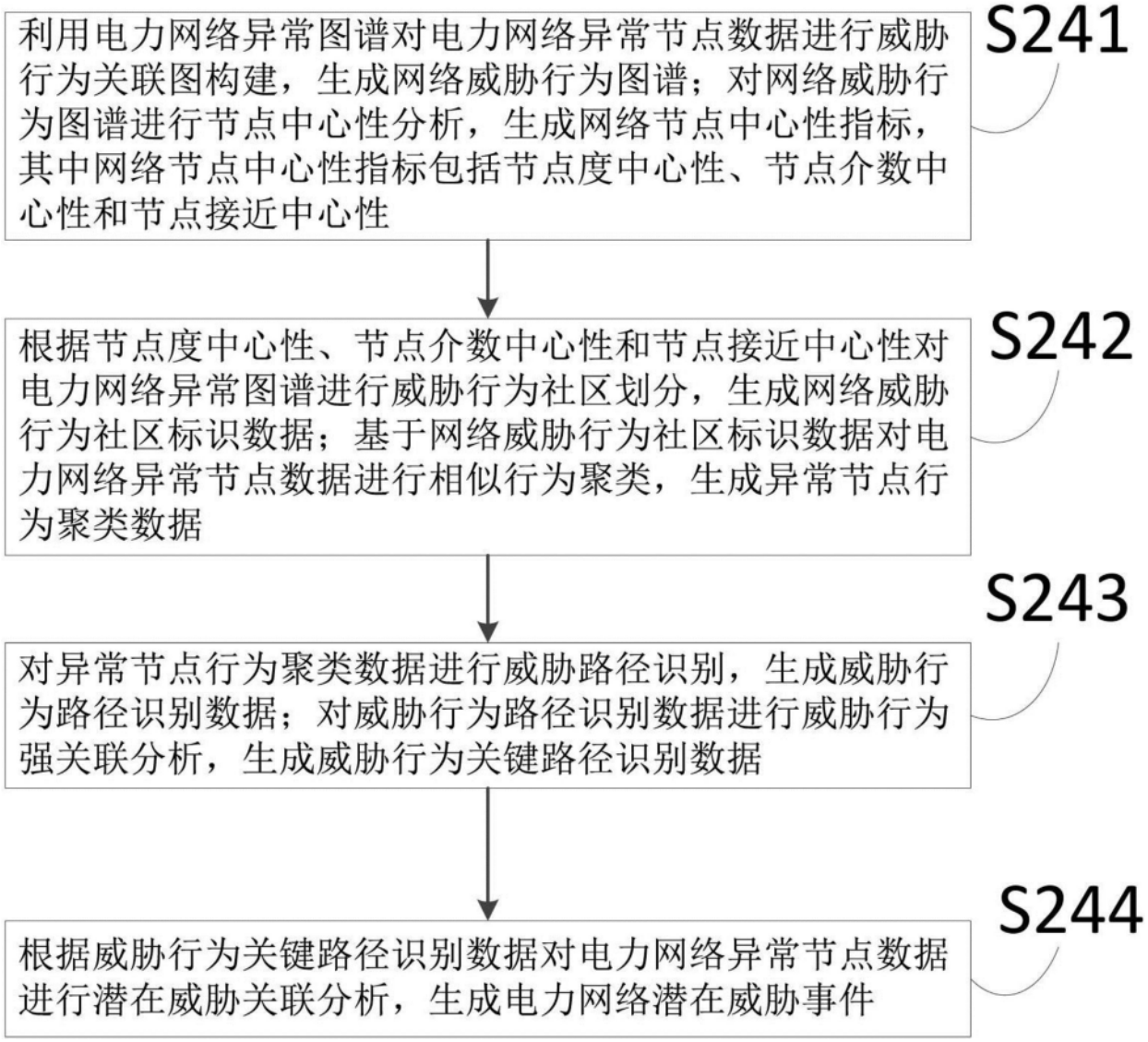

S241
利用电力网络异常图谱对电力网络异常节点数据进行威胁行为关联图构建，生成网络威胁行为图谱；对网络威胁行为图谱进行节点中心性分析，生成网络节点中心性指标，其中网络节点中心性指标包括节点度中心性、节点介数中心性和节点接近中心性
S242
根据节点度中心性、节点介数中心性和节点接近中心性对电力网络异常图谱进行威胁行为社区划分，生成网络威胁行为社区标识数据；基于网络威胁行为社区标识数据对电力网络异常节点数据进行相似行为聚类，生成异常节点行为聚类数据
S243
对异常节点行为聚类数据进行威胁路径识别，生成威胁行为路径识别数据；对威胁行为路径识别数据进行威胁行为强关联分析，生成威胁行为关键路径识别数据
S244
根据威胁行为关键路径识别数据对电力网络异常节点数据进行潜在威胁关联分析，生成电力网络潜在威胁事件

图3

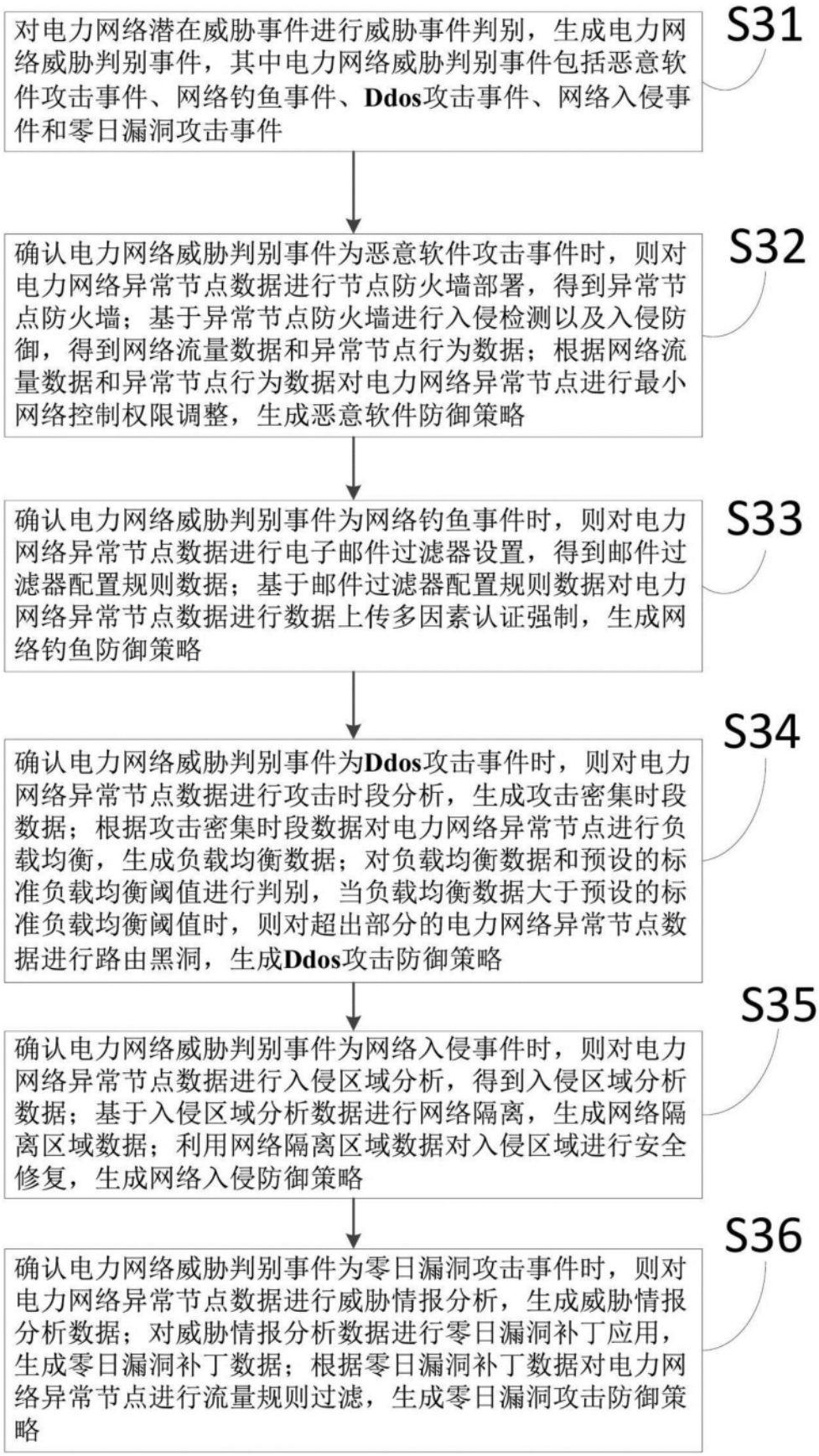

S31
对电力网络潜在威胁事件进行威胁事件判别，生成电力网络威胁判别事件，其中电力网络威胁判别事件包括恶意软件攻击事件、网络钓鱼事件、Ddos攻击事件、网络入侵事件和零日漏洞攻击事件
S32
确认电力网络威胁判别事件为恶意软件攻击事件时，则对电力网络异常节点数据进行节点防火墙部署，得到异常节点防火墙；基于异常节点防火墙进行入侵检测以及入侵防御，得到网络流量数据和异常节点行为数据；根据网络流量数据和异常节点行为数据对电力网络异常节点进行最小网络控制权限调整，生成恶意软件防御策略
S33
确认电力网络威胁判别事件为网络钓鱼事件时，则对电力网络异常节点数据进行电子邮件过滤器设置，得到邮件过滤器配置规则数据；基于邮件过滤器配置规则数据对电力网络异常节点数据进行数据上传多因素认证强制，生成网络钓鱼防御策略
S34
确认电力网络威胁判别事件为Ddos攻击事件时，则对电力网络异常节点数据进行攻击时段分析，生成攻击密集时段数据；根据攻击密集时段数据对电力网络异常节点进行负载均衡，生成负载均衡数据；对负载均衡数据和预设的标准负载均衡阈值进行判别，当负载均衡数据大于预设的标准负载均衡阈值时，则对超出部分的电力网络异常节点数据进行路由黑洞，生成Ddos攻击防御策略
S35
确认电力网络威胁判别事件为网络入侵事件时，则对电力网络异常节点数据进行入侵区域分析，得到入侵区域分析数据；基于入侵区域分析数据进行网络隔离，生成网络隔离区域数据；利用网络隔离区域数据对入侵区域进行安全修复，生成网络入侵防御策略
S36
确认电力网络威胁判别事件为零日漏洞攻击事件时，则对电力网络异常节点数据进行威胁情报分析，生成威胁情报分析数据；对威胁情报分析数据进行零日漏洞补丁应用，生成零日漏洞补丁数据；根据零日漏洞补丁数据对电力网络异常节点进行流量规则过滤，生成零日漏洞攻击防御策略

图4