现代电力
MODERN ELECTRIC POWER
■ 中国高校优秀科技期刊 ■ 全国中文核心期刊
■ 中国科技核心期刊 ■ 中国知网收录期刊
■ 万方数据收录期刊 ■ 《CAJ-CD规范》执行优秀期刊

电力监控系统网络安全管理平台端点Agent体系架构及关键技术

马骁 崔旭东 李勃 高明慧 马力 赵航

Power Monitoring System Network Security Management Platform Endpoint Agent Architecture and Key Technologies

MA Xiao, CUI Xudong, LI Bo, GAO Minghui, MA Li, ZHAO Hang

引用本文:
马骁, 崔旭东, 李勃, 等. 电力监控系统网络安全管理平台端点Agent体系架构及关键技术[J]. 现代电力, 2023, 40(6): 1023-1031. DOI: 10.19725/j.cnki.1007-2322.2022.0124
MA Xiao, CUI Xudong, LI Bo, et al. Power Monitoring System Network Security Management Platform Endpoint Agent Architecture and Key Technologies[J]. Modern Electric Power, 2023, 40(6): 1023-1031. DOI: 10.19725/j.cnki.1007-2322.2022.0124

在线阅读 View online: https://doi.org/10.19725/j.cnki.1007-2322.2022.0124

文章编号：1007-2322(2023)06-1023-09 文献标志码：A 中图分类号：TM73

电力监控系统网络安全管理平台端点 Agent 体系架构及关键技术

马骁[1,2]，崔旭东[1,2]，李勃[1,2]，高明慧[1,2]，马力[1,2]，赵航[1,2]
（1. 南瑞集团有限公司 (国网电力科学研究院有限公司), 江苏省 南京市 211106；
2. 北京科东电力控制系统有限责任公司, 北京市 海淀区 100192）

Power Monitoring System Network Security Management Platform Endpoint Agent Architecture and Key Technologies

MA Xiao[1,2]，CUI Xudong[1,2]，LI Bo[1,2]，GAO Minghui[1,2]，MA Li[1,2]，ZHAO Hang[1,2]
（1. NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, Jiangsu Province, China；
2. Beijing Kedong Electric Power Control System Co., Ltd., Haidian District, Beijing 100192, China）

摘要：为了进一步提升网络安全监测能力，国家电网公司制定了资产及行为数据全采集的工作目标，针对工作目标和目前端点 Agent 存在的系统事件采集不全、采集项少且不规范、技术架构不清晰等问题，应用端点检测与响应技术，重构原端点 Agent 的体系架构，制定新的端点系统信息采集规范，突破系统信息采集、系统事件订阅、系统资源占用监视和限制等关键技术，研发了新的端点 Agent 产品。经实验验证，重构后的端点 Agent 性能和系统资源占用满足监测能力提升要求。最后对端点 Agent 和端点检测与响应技术在电力监控系统的应用前景做出展望。

关键词：电力监控系统；网络安全；端点检测与响应；Agent

Abstract： In order to further improve the capabilities to monitor the network security, the State Grid Corporation of China formulated the work goal of full collection of asset and behavior data, applied endpoint detection and response technology, reconstructed the architecture of the original endpoint agent, formulated new endpoint system information collection specifications, and break through key technologies such as endpoint system information collection, system event subscription, system resource consumption monitoring and throttling, And then new endpoint agent product was developed. After experimental verification, the reconfigured endpoint agent performance and system resource occupation meet the requirements for monitoring capability improvement. Finally, the application prospect of endpoint agent and endpoint detection and response technology in power monitoring system is prospected.

Keywords： power monitoring system；network security；endpoint detection and response；Agent

DOI：10.19725/j.cnki.1007-2322.2022.0124

0 引言

近年来，随着信息技术的发展，网络安全攻击手段花样翻新，未知威胁攻击、0day 漏洞攻击、高级持续性威胁 (advanced persistent threat，APT) 攻击层出不穷，网络攻击更有针对性、隐蔽性和持久性。针对电力基础设施的网络攻击事件频发[1]，有组织、成体系的网络对抗行为已经上升到国家安全的层面。

国家安全法、网络安全法，数据安全法、网络安全等级保护条例、关键基础设施保护条例等相继颁布实施，国家对网络安全的重视程度前所未有，电力系统网络安全面临挑战[2-5]。2017 年，国家电网公司印发 1084 号文 (国家电网公司关于加快推进电力监控系统网络安全管理平台建设的通知)，根据通知要求，组织研发了电力监控系统网络安全管理平台 (简称安管平台) 等软件和硬件设备。按照设备自身直接感知、监测装置分布采集、监管平台统一管控的原则，构建设备、监测装置、监管平台三层结构的国家电网公司网络安全监管体系，已全面投入使用，并取得了良好的效果。

Gartner 在 2013 年首次提出端点检测与响应 (endpoint detection and response，EDR)[6]，EDR 通过持续自适应风险与信任评估 (continuous adaptive risk and trust assessment，CARTA)[7] 从预防、检测、

响应和预测 4 个阶段持续地应对网络空间威胁。国内有齐安信、深信服、绿盟等[8]，国外有 Comodo、Kaspersky、Fireye 等[9-10]网络安全厂商都推出了 EDR 产品，但其为通用型商业产品，并不能在复杂的电力系统中直接使用。

安管平台作为针对电力系统深度定制的网络安全产品，在复杂的电力系统中实现了安全信息与事件管理 (security information and event management, SIEM)[11]，但其对未知威胁攻击检测和响应能力偏弱，已经不能满足电力系统网络安全的需要，亟需改进。在 SIEM 的基础上，应用 EDR 技术为安管平台提供 CARTA 能力，应对日益严峻的网络安全威胁会是一个与时俱进的解决方案[12]。

这里提到的网络空间资产即端点，是指在网络空间中以 IP 地址为基础包括主机设备、网络设备、安防设备等真实客观存在的主体。根据管控强度，分为强管控端点和弱管控端点，强管控是指端点内部和外部行为都需要被监视；弱管控是指端点仅能被间接监视其外部行为，强管控端点通过端点 Agent 实现强管控。

本文针对资产及行为数据全采集工作目标中，强管控端点采集什么和如何采集的问题，以及现有的安管平台 Agent 存在系统事件采集不全、采集项少且不规范、技术架构不清晰等问题。应用 EDR 技术，重构端点 Agent 的体系架构，重构安管平台 Agent 为 EDR Agent，制定端点系统信息采集规范。突破端点系统信息采集、系统事件订阅、系统资源占用监视和限制等关键技术。实现所采集的系统信息结构化和规范化、采集项和采集方式深度可配置、系统资源占用自适应，以支撑安管平台 EDR 改造。

1 EDR Agent 体系架构

1.1 总体设计

EDR Agent 是部署在电力监控系统强管控端点的轻量级软件，其对安管平台 Agent 的体系架构进行重新设计，来解决系统信息如何采集的问题，实现采集项和采集周期可配置、系统安全事件不丢失、系统资源占用可限制、系统结构模块化等特性，图 1 描述了 EDR Agent 的体系架构。同时，端点系统信息采集规范对采集什么系统信息提出要求，遵照采集规范监管平台通过配置下发来定义系统中的实际采集项。

1）系统事件订阅。系统事件订阅功能采用发布者–订阅者模式，发布者与端点系统紧密结合，采集 Inotify、Linux Audit 等系统服务事件。一个发布者可以有多个订阅者，订阅者根据具体需求订阅发布者发布的系统事件信息，并将订阅的系统事件保存到端点数据库供系统信息采集功能查询使用。

同时，系统事件订阅功能监视端点数据库，按照配置定义的系统事件保存时间，清理冗余数据。

2）系统暂态信息。系统暂态信息是指端点系统当前的瞬时的状态信息，其按照表的方式分类组织，表是虚拟的，是一个逻辑结构，并不是物理存在的表。表通过 SQL 语句进行查询操作，EDR Agent 将 SQL 语句转化为对应的系统命令调用、系统 API 调用或系统配置文件读取等操作，然后返回结果。

同时，系统暂态信息的查询结果会作为快照保存到端点数据库，系统信息采集功能进行查询时，刷新端点数据库中的快照。

3）系统信息采集。系统信息采集功能是 EDR Agent 的核心功能，调度查询系统信息。系统信息采集过程分为：系统信息查询过程、系统事件查询过程和系统暂态信息查询过程。

系统信息查询过程，第三方应用程序通过规范的接口调用采集系统信息，通过 EDR Agent 采集系统信息可以避免产生过大的暴露面。

系统事件查询过程，按照调度规则查询已保存到端点数据库的系统事件，其根据游标位置定位采集开始点，格式化后上报到消息总线。

系统暂态信息查询过程，按照调度规则分为全量获取和差异对比。全量获取过程查询虚拟表，格式化后上报到消息总线。差异对比过程查询虚拟表后，需要与端点数据库中的快照对比，只上报差异信息。差异对比过程另一个主要用途是可以定义非瞬逝的行为事件，比如：新增、删除用户。可以根据配置规则每 300 s 查询一次用户信息表，与快照对比出现差异时，即为行为事件进行上报。

4）其他组件与 EDR Agent 交互。在电力监控系统网络安全监测体系中，监管平台对 EDR Agent 集中管控，下发配置信息，EDR Agent 通过消息总线向监测装置上报网络安全信息和事件。

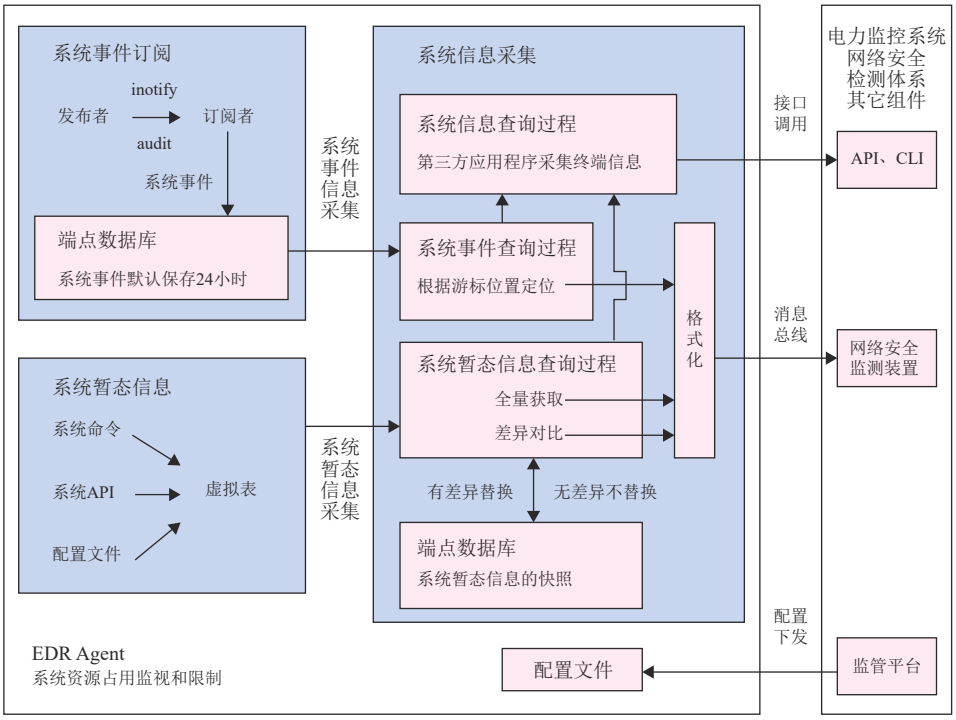

图 1　EDR Agent 的体系架构

Fig. 1　Architecture of the EDR Agent

EDR Agent 的目标是作为电力监控系统网络安全端点信息采集的标准组件，部署到电力监控系统端点设备上采集系统信息。提供命令行接口(command line interface，CLI) 和 C、Python、Java 等应用程序编程接口以使第三方应用程序可以通过 EDR Agent 采集端点信息。

1.2　进程和线程设计

图 2 描述了 EDR Agent 应用程序进程和线程之间的逻辑关系。

1）主进程。主进程读取配置文件、启停子线程、维护端点数据库中的数据。EDR Agent 不能影响系统正常业务的运行，系统信息采集子进程的某些查询可能会占用大量系统资源，所以要对 EDR Agent 的系统资源占用做出限制，系统资源占用监视和限制功能运行于主进程，其监视系统资源占用情况，并根据配置要求做出相应处理。

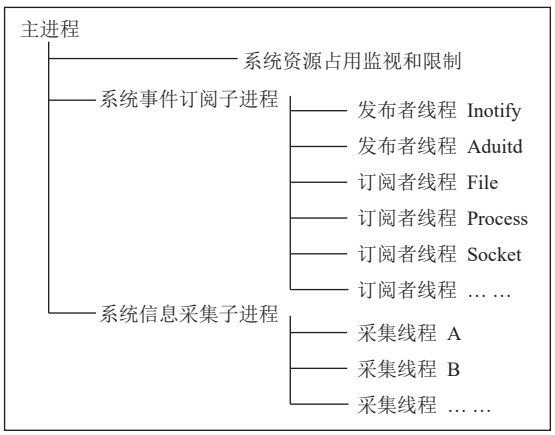

图 2　EDR Agent 进程和线程设计

Fig. 2　EDR Agent process and thread design

2）系统事件订阅子进程。系统事件订阅子进程启停相关线程。系统事件订阅采用发布者–订阅者模式，每个发布者或订阅者分别对应一个线程。

3）系统信息采集子进程。系统信息采集子进程运行调度职能，根据配置启动多个线程进行查询，每个线程对应一个查询。

1.3　端点系统信息采集规范

国家电网公司 1084 号文中规定了主站和厂站的服务器、工作站等端点设备的采集项。但随着对电力监控系统网络安全防护要求的提高，出现系统信息采集深度不足、采集项的分类不规范等问题，所以在国家电网公司 1084 号文的基础上重新定义了端点系统信息采集规范。

新的采集规范在增加采集项的基础上，对采集的端点系统信息进行面向对象抽象建模，将采集项分为 12 类，每类采集项分为更为具体的采

集对象，每个采集对象有其属性，表 1 描述了端点系统信息采集对象。采集对象是系统信息采集的基本单元，采集对象按采集方式不同分为周期调阅和事件触发，周期调阅按照配置的周期上报系统信息，由系统暂态信息查询全量获取过程支撑。事件触发即事件发生即上报，由系统暂态信息查询差异对比过程和系统事件查询过程支撑。

表 1 端点系统信息的采集对象

Table 1 The collection object of endpoint system information

分类	采集对象举例	采集对象属性举例	采集方式
进程信息	进程基本信息	进程名、进程ID	周期调阅
文件信息	文件权限变更	文件名、文件大小	事件触发
系统配置	基础信息	系统厂商、内核版本	周期调阅
服务信息	系统服务列表	服务名、安装时间	周期调阅
驱动信息	驱动列表	驱动名、厂商	周期调阅
硬件配置	CPU	架构、品牌	周期调阅
硬件状态	CPU	占用率、温度	周期调阅
软件信息	软件基本信息	安装包名、安装时间	周期调阅
用户信息	用户属性变更	用户名、用户ID	事件触发
外设信息	USB接入接出	USB接口号、厂商	事件触发
网络信息	IP信息	IP地址、MAC地址	事件触发
会话信息	主机会话列表	用户名、登录方式	周期调阅

在国家电网公司 1084 号文定义的采集规范基础上，新增 42 个采集项，共梳理 75 个采集对象。表 1 中硬件配置和硬件状态分类都包括 CPU 采集对象，但其所指不同， CPU 硬件配置采集对象包括架构 (x86_x64)、品牌 (intel) 等属性，CPU 硬件状态采集对象包括占用率 (40%)、温度 (70℃) 等属性。

2 EDR Agent 关键技术

2.1 系统信息采集技术

系统信息采集是 EDR Agent 的核心功能，其负责调度采集作业，将采集到的系统信息格式化后通过消息总线上报给监测装置，需要解决调度、结构化存储和查询、差异对比和格式化上报等问题。图 3 描述了系统信息采集流程。

系统信息采集进程是 EDR Agent 的子进程，启动后根据配置为每条查询分别建立一个采集线程。采集线程根据采集对象的采集方式和事件来源不同，分为 3 种处理过程：

系统暂态信息查询全量获取过程，对应周期调阅的采集方式，SQL 语句查询虚拟表，首先对 SQL 语句解析以获取系统信息，以表格形式返回的系统信息经过格式化后上报到消息总线。

系统暂态信息查询差异对比过程，对应事件触发采集方式，其事件来源为系统暂态信息。同样，SQL 语句查询虚拟表，对 SQL 语句解析以获取系统信息。系统信息以表格形式返回后，与快照对比，无差异则不做处理进入下个采集周期，有差异则替换原快照，经格式化后上报到消息总线。

系统事件查询过程，对应事件触发采集方式，其事件来源为系统事件订阅，系统事件订阅信息已经保存到端点数据库，只需要查询数据库中的表就可以，查询结果经格式化上报到消息总线。

如第三方应用程序调用系统信息采集功能接口，查询结果直接返回给第三方应用程序，其根据自身的业务逻辑进行处理。

1 ）系统信息采集配置。采集对象配置包括查询语句、查询间隔、格式化方式等信息，部分采集对象配置如表 2 所示，实际的配置文件为 JSON 格式。

2）端点数据库系统。端点数据库系统负责保存系统信息及提供系统信息的 SQL 查询功能，涉及到 SQL 解析、数据存储和虚拟表，这里以 3 个开源免费的组件 Lemon Parser、RocksDB 和 rrrdb 为基础，并结合程序逻辑实现的虚拟表来支撑端点数据库系统的实现。图 4 展示了端点数据库系统 SQL 语句的处理过程。

SQL 解析由分词器和解析器组成，分词器处理 SQL 语句字符串，将给定的 SQL 字符串标记为一组标记，然后解析器从这组标记中构建一个抽象语法树 (abstract syntax tree，AST) [13]。

规划执行器获得 SQL 解析器生成的 AST，构建一个计划。比如，有一个 SQL 语句 SELECT * FROM users WHERE uid = 1001，规划器生成一个计划来获取具有 uid = 1001 的数据。

数据存储中的数据通过规划执行器直接获取，而虚拟表的数据通过系统命令调用、系统 API 调用或系统配置文件以程序逻辑获取。此端点数据库系统在性能方面还有很大的优化空间，比如数据格式、缓存、批量操作等，未来有机会进行专项研究。

3）关联查询。SQL 语句可以进行多表关联

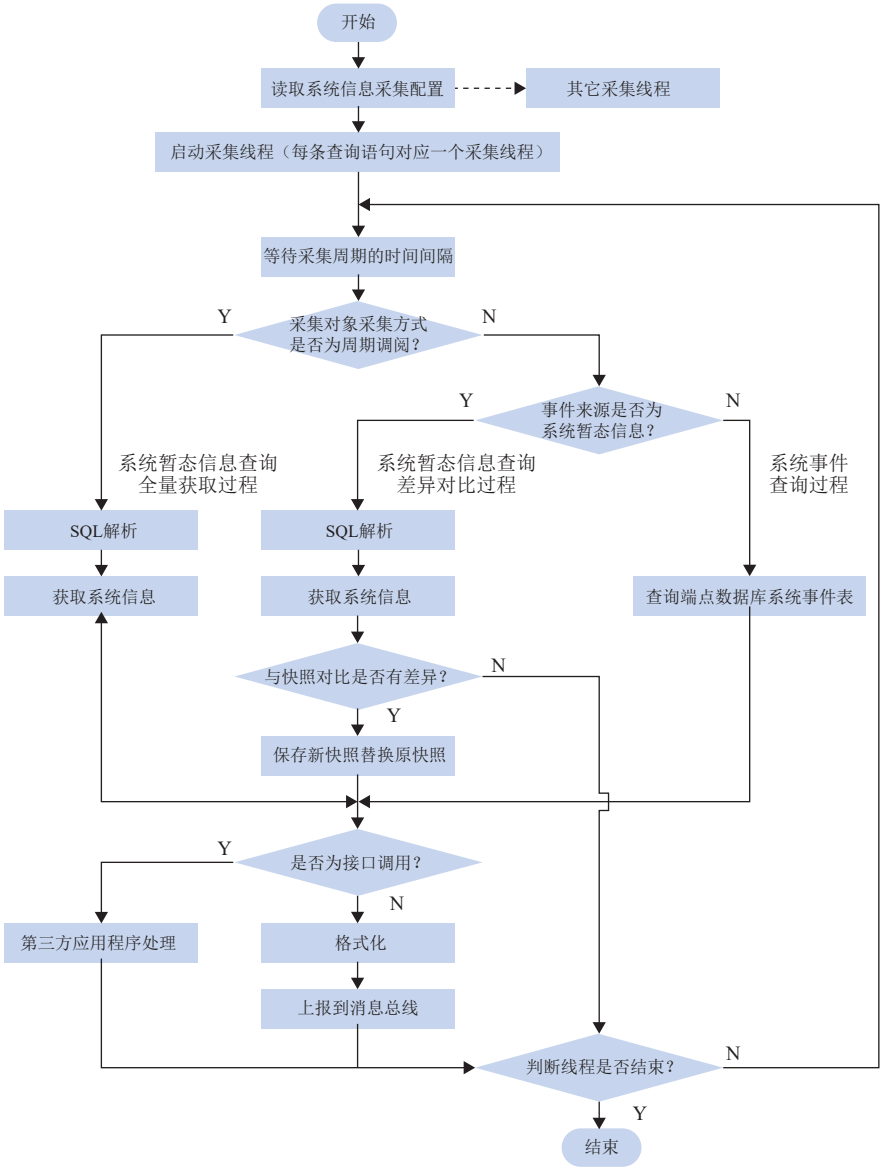

图 3　系统信息采集流程

Fig. 3　System information collection process

表 2　采集对象配置

Table 2　The configuration of the collection object

采集对象	查询语句	查询间隔	采集过程	格式化方式
文件权限变更	SELECT * FROM file_events;	10	系统事件查询过程	通用告警格式
用户属性变更	SELECT * FROM users;	60	系统暂态信息查询差异对比过程	通用告警格式
CPU硬件状态	SELECT * FROM cpu_status;	1	系统暂态信息查询全量获取过程	通用告警格式

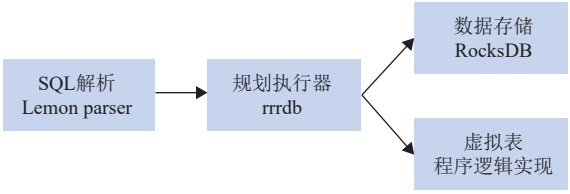

图 4　SQL 语句处理过程

Fig. 4　SQL statement processing

查询，比如关联 CPU 硬件状态表和 CPU 硬件信息表，可以得到更详尽的 CPU 信息。虽然目前的采集对象信息仅从一张表中获取即可，无需进行关联查询，但第三方应用程序可以使用关联查询获得结构化更好的端点系统信息。但需要注意的是，系统暂态信息虚拟表和系统事件数据表关联时数据实效的问题，以及查询性能等问题。

4）格式化上报。格式化上报功能采用可替换组件的方式，目前实现的组件将采集到的信息转化为电力系统通用告警格式[14]上报到消息总

线。其中，某些采集对象由其变更前和变更后的信息组成，所以需要组合本次查询信息和以往快照信息经组合格式化后上报到消息总线。比如：用户名变更这个采集对象上报时需要包括变更前用户名和变更后用户名。

2.2 系统事件订阅技术

系统事件订阅利用系统服务获取系统事件，其采用发布者–订阅者模式，发布者与端点系统紧密结合，采集系统服务的事件，订阅者按需订阅发布者发布的系统事件，解决瞬逝系统事件遗失的问题。图 5 描述了系统服务、发布者、订阅者、端点数据库表和采集对象的对应关系。

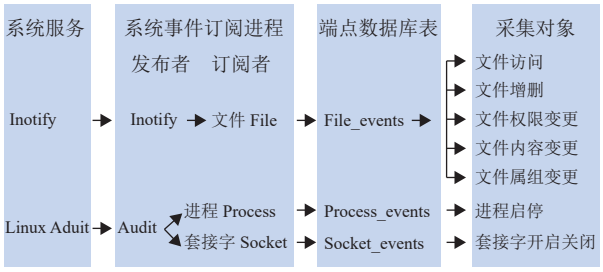

图 5 系统服务、发布者、订阅者、端点数据库表和采集对象的对应关系

Fig. 5 Correspondence between system services, publishers, subscribers, endpoint database tables, and collection objects

Inotify 系统服务于 Linux 2.6.13 版本加入 Linux 内核，它提供了一种监视文件系统事件的机制，监视文件的添加、删除、移动、修改等各种事件，通过此机制内核空间事件可以立即通知给用户空间应用程序[15]。Linux Audit 系统服务于 Linux 2.6 版本加入 Linux 内核，它用于收集记录系统、内核、用户进程发生的安全事件。该子系统可以可靠地收集系统事件信息，帮助跟踪在系统上执行过的一些操作[16]。除现有的 Inotify 和 Linux Audit 外，后续系统事件订阅功能会考虑加入 Udev 等系统服务作为发布者，以便能够更及时得知内核或底层硬件设备发生了什么。

订阅者订阅的系统事件保存到端点数据库以提供给系统信息采集功能使用，表 3 以 file_events 为例描述了端点数据库中系统事件表的结构。

2.3 系统资源占用监视和限制技术

生产环境中，为了防止 EDR Agent 在采集系统信息时占用过多的系统资源，从而影响常规业务运行，通过引入系统资源占用监视和限制功能实现自适应系统资源占用，称其为 Watchdog。

表 3 File_events 端点数据库表结构

Table 3 Endpoint database table structure of file_events

字段名	描述	示例
target_path	文件所在路径	/opt/edr.conf
action	文件系统事件	create
inode	文件系统inode编号	394820
uid	文件属主ID	0
gid	文件属组ID	0
mode	文件的访问权限	0644
size	文件大小，单位字节	15
atime	文件最后访问时间	1644905410
mtime	文件最后修改时间	1644905410
ctime	文件属性最后修改时间	1644905410

Watchdog 会监视系统信息采集子进程的内存和 CPU 占用情况，如果超出了设定的阈值将强制终止此子进程以释放占用的系统资源，图 6 描述系统资源占用监视和限制流程。

然而系统超出阈值会有各种原因，不能一概而论，重启几次被终止的子进程，继续监测其资源占用情况，经过多次重启系统资源占用依旧超过阈值。最终不再重新启动，输出错误信息并告警。

表 4 描述 watchdog 相关配置，其分为两部分，一部分是关于内存和 CPU 相关阈值的设定，另一部分是关于系统信息采集子进程启动及重启等相关的设定，从而使监视和限制系统资源更加灵活可控。其中占用 CPU 百分比阈值、CPU 整体占用百分比阈值、超出阈值持续时长这几个配置项是与的关系。

3 实验和分析

3.1 实验数据

实验环境包括设备、监测装置和监管平台，监测装置和监管平台采用北京科东公司研发的相关产品。设备硬件配置为 Intel i5 4 核心 CPU 和 4G 内存，操作系统为 Ubuntu 20.04。根据端点采集对象不同，采集周期从 1s 到 300 s 不等，平均采集周期为 20 s 左右。为避免浪涌，可以将各采集对象的采集周期进行错位配置，比如采集周期同为 20 s 的采集对象分别配置为 19、20、21 s。

相同软硬件环境下原安管平台 Agent 的 CPU 占用率为 4%、内存占用为 40m。其相当于有 33 个 EDR Agent 采集对象，对应 EDR Agent 的 CPU

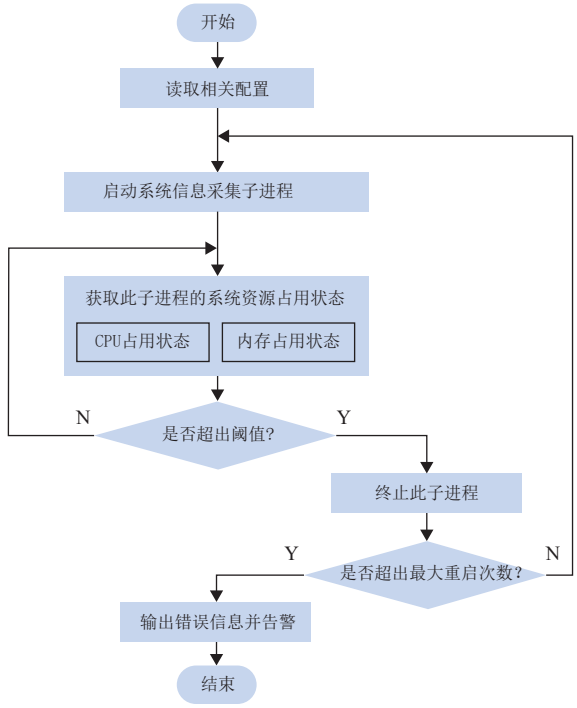

图 6　系统资源占用监视和限制流程

Fig. 6　System resource consumption monitoring and throttling processes

表 4　系统资源占用监视和限制相关配置

Table 4　System resource consumption monitoring and throttling related configurations

配置项	描述	默认值
enable	Watchdog是否启用	true
memory_threshold	占用内存的阈值	80m
cpu_threshold	占用CPU百分比阈值	10%
cpu_system_threshold	CPU整体占用百分比阈值	85%
cpu_latency_threshold	超出阈值持续时长	20s
start_delay	启动多久开始进行资源占用监视	20s
restart_times	自动重新启动的次数	10
restart_interval	自动重启计数时间范围	300s
restart_delay	自动重新启动延时	5s

占用率为 1.5%、内存占用为 30m，EDR Agent 资源占用优于原安管平台 Agent。

表 5 根据不同的采集对象数目和平均采集周期，统计 EDR Agent 系统资源占用情况。全采集 75 个采集对象，系统资源 CPU 占用率 4.9%、内存占用 60m，在生产环境中安装有 EDR Agent 的设备硬件配置会比这个高，实验结果符合预期。

系统频繁操作会产生大量系统事件，从而消耗系统资源，Watchdog 会在系统资源占用超过阈值时重启系统信息采集子进程。

表 5　EDR Agent 测试数据

Table 5　EDR Agent test data

采集对象数目	平均采集周期/s	CPU占用率/%	内存占用/ m
33	3	10.9	30
33	7	4.5	30
33	10	2.9	30
33	20	1.5	30
56	3	34.1	50
56	7	14.7	50
56	10	10.6	50
56	20	5.4	50
75	3	38.2	60
75	7	16.3	60
75	10	11.8	60
75	20	4.9	60

Watchdog 实验中设定采集对象数目 75 个，平均采集周期 10s，总体 CPU 占用阈值 50%，使应用程序进行大量新建、读写、修改文件操作，使总体 CPU 占用超过阈值 50%，此时系统信息采集子进程会持续重启以节省系统资源，直至总体 CPU 占用低于 50% 的阈值，实验结果符合预期。

3.2　EDR Agent 相比安管平台 Agent 的改进

1）重构技术架构。采用结构化数据表示方法，将端点系统信息抽象为对象，表现为虚拟表和数据库表，其可以通过 SQL 进行查询；通过监管平台下发采集项和调度方式来统筹配置，保证 Agent 核心功能稳定的同时，增加灵活性；采用差异对比和全量获取相结合的系统信息采集方式，得以节省消息总线带宽；通过系统资源占用监视和限制技术管控系统资源的占用；提供系统信息查询接口供第三方应用程序调用。

2）优化采集技术。原安管平台 Agent 以事件触发方式上报的系统事件，其和周期轮询上报的系统事件一样也是通过守护进程周期循环采集得到，只是采集周期比较短，会存在一个轮询周期内的瞬逝变化无法获取的问题，如采集周期设置的过短又会出现性能问题。EDR Agent 采用 Linux Audit、Inotify 系统内核机制进行事件采集，节省对系统资源占用，提高准确性，解决瞬逝系统事件遗失的问题。

3）扩充采集项。在国家电网公司 1084 号文基础上，新增 42 个采集项，共梳理 75 个采集对象，如新增了进程、文件等采集对象及其属性。

3.3 端点安全展望

端点安全新技术不断涌现[17]，统一端点安全(unified endpoint security，UES)融合防病毒软件(anti-virus software，AV)、端点防护平台(endpoint protection platform，EPP)、EDR以及扩展检测与响应(extended detection & response，XDR)。UES Agent在EDR Agent基础上承担更多的网络安全功能，除EDR Agent功能外还包括：基线核查、漏洞扫描、恶意代码检测、阻断、可信计算等功能。最终，电力监控系统只需要安装一个端点Agent，无需多头安装、多头配置、多头管理，形成一站式的电力监控系统网络安全端点Agent解决方案。

同时，应该认识到电力监控系统网络安全数据采集具有数据量大、种类多样、主站和厂站地域分布广等特点。基于网络安全数据的全采集，实现网络安全威胁事件的全发现，尤其是安管平台服务端还有很多技术需要突破，如：面对复杂电力系统环境，大数据量的传输、存储、分析、挖掘和实时处理。如何应用对抗战术技术和常识(adversarial tactics techniques & common knowledge，ATT&CK)[18]、网络安全对策知识图谱(D3FEND)、安全编排自动化与响应(security orchestration, automation and response，SOAR)[19]、用户实体行为分析(user & entity behavior analysis，UEBA)[20]等技术，关联威胁情报(threat intelligence，TI)以实现更精准、更智能的网络安全事件检测以及响应，是下一步亟需研究和解决的问题。

进一步，结合美国国家标准与技术研究所(National Institute of Standards and Technology，NIST)、国防高级研究计划局(Defense Advanced Research Projects Agency，DARPA)、Mitre、Gartner等研究机构提出的安全框架和方法论提升电力系统网络安全，也是需要研究和思考的问题。

4 结语

EDR Agent是原安管平台Agent的升级改造，解决现有的安管平台Agent存在系统事件采集不全、采集项少且不规范、技术架构不清晰等问题。本文论述了EDR Agent的体系架构和端点系统信息采集规范，并对系统信息采集、系统事件订阅、系统资源占用监视和限制等关键技术进行讨论。结合监测装置、监管平台进行实验验证，取得了良好的效果。

未来，尤其是十四五期间，EDR Agent将作为安管平台的标准组件，部署到电力系统各主站和厂站强管控端点设备上，适配凝思、麒麟等国产操作系统。通过对端点信息的深度采集，实时上报端点网络安全相关的信息，为EDR的检测与响应提供数据支撑。

参考文献

[1] 黄鑫, 陈德成, 孙军, 等. 网络攻击下电力系统信息安全研究综述[J]. 电测与仪表, 2017, 54(23): 68−74.
HUANG Xin, CHEN Decheng, SUN Jun, *et al*. A review of information security research in power system under cyber attack[J]. Electrical Measurement & Instrumentation, 2017, 54(23): 68−74(in Chinese).

[2] 王栋, 陈传鹏, 颜佳, 等. 新一代电力信息网络安全架构的思考[J]. 电力系统自动化, 2016, 40(2): 6−11.
WANG Dong, CHEN Chuanpeng, YAN Jia, *et al*. Pondering a new-generation security architecture model for power information network[J]. Automation of Electric Power Systems, 2016, 40(2): 6−11(in Chinese).

[3] 王恒, 辛耀中, 尚学伟, 等. 智能电网调度控制系统数据总线技术[J]. 电力系统自动化, 2015, 39(1): 9−13.
WANG Heng, XIN Yaozhong, SHANG Xuewei, *et al*. A new data bus technology for smart grid dispatching and control systems[J]. Automation of Electric Power Systems, 2015, 39(1): 9−13(in Chinese).

[4] 辛耀中, 石俊杰, 周京阳, 等. 智能电网调度控制系统现状与技术展望[J]. 电力系统自动化, 2015, 39(1): 2−8.
XIN Yaozhong, SHI Junjie, ZHOU Jingyang, *et al*. Technology development trends of smart grid dispatching and control systems[J]. Automation of Electric Power Systems, 2015, 39(1): 2−8(in Chinese).

[5] 张晓, 李伟, 高明慧, 等. 基于树模型的电力监控系统链路信息管理[J]. 电力系统自动化, 2016, 40(11): 126−131.
ZHANG Xiao, LI Wei, GAO Minghui, *et al*. Tree model based link information management for power monitoring system[J]. Automation of Electric Power Systems, 2016, 40(11): 126−131(in Chinese).

[6] Gartner. Named: Endpoint Threat Detection & Response[EB/OL]. [2013-7-26].https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/.

[7] Gartner. Build Adaptive Security Architecture Into Your Organization[EB/OL]. [2017-6-30]. https://www.gartner.

com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/.

[8] 刘飞, 黄云婷, 江巍, 等. 端点威胁检测与响应技术研究及发展研判[J]. 通信技术, 2020, 53(09): 2271−2275.
LIU Fei, HUANG Yunting, JIANG Wei, *et al*. Research and development of endpoint threat detection and response technology[J]. Communications Technology, 2020, 53(09): 2271−2275(in Chinese).

[9] Gartner. Market Guide for Endpoint Detection and Response Solutions[EB/OL]. [2019-12-23].https://www.gartner.com/en/documents/3978685.

[10] Gartner. Solution Comparison for Endpoint Detection and Response Technologies and Solutions[EB/OL]. [2020-1-31].https://www.gartner.com/en/documents/3980362.

[11] 李艳斐, 李斯祺. 基于SIEM的APT检测与防御体系研究[J]. 网络空间安全, 2018, 9(06): 16−19+25.
LI Yanfei, LI Siqi. Research on APT detection and defense system based on SIEM[J]. Cyberspace Security, 2018, 9(06): 16−19+25(in Chinese).

[12] 褚龙, 伍荣, 龙飞宇. 端点检测与响应技术及其发展趋势[J]. 通信技术, 2017, 50(7): 1493−1498.
CHU Long, WU Rong, LONG Feiyu. Endpoint detection and response technology and its development[J]. Communications Technology, 2017, 50(7): 1493−1498(in Chinese).

[13] 崔娜. 面向数据库性能的SQL语句解析与翻译[J]. 现代电子技术, 2016, 39(11): 99−102+107.
CUI Na. SQL parse and translation oriented to database performance[J]. Modern Electronics Technique, 2016, 39(11): 99−102+107(in Chinese).

[14] GB/T 31992—2015, 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. 电力系统通用告警格式[S].

[15] 武特, 陈莉君. 基于inotify的内核态与用户态跨平台数据交互[J]. 西安邮电学院学报, 2012, 17(04): 79−82.
WU Te, CHEN Lijun. Cross-platform data exchange based on inotify between kernel mode and user mode[J]. Journal of Xi· An University of posts and telecommunications, 2012, 17(04): 79−82(in Chinese).

[16] Selectel. Auditing System Events in Linux[EB/OL]. [2017-6-8].https://blog.selectel.com/auditing-system-events-linux

[17] Gartner. Hype Cycle for Endpoint Security[EB/OL]. [2020-7-15].https://www.gartner.com/en/documents/3987589

[18] 何树果, 袁瑗, 朱震, 等. 基于ATT&CK框架的域威胁检测[J]. 信息技术与网络安全, 2021, 40(12): 15−18+25.
HE Shuguo, YUAN Yuan, ZHU Zhen, *et al*. Domain threat detection based on ATT&CK framework[J]. Information Technology and Networks Security, 2021, 40(12): 15−18+25(in Chinese).

[19] 赵粤征, 叶建伟, 贠珊, 等. 基于SOAR的安全运营自动化关键技术构建及未来演进方向[J]. 信息技术与网络安全, 2021, 40(03): 19−27.
ZHAO Yuezheng, YE Jianwei, YUN Shan, *et al*. Key technology construction and future evolution direction of security operation automation based on SOAR[J]. Information Technology and Networks Security, 2021, 40(03): 19−27(in Chinese).

[20] 刘进, 李江波, 叶兵. 对于UEBA数据安全内控风险管理的研究[J]. 网络空间安全, 2021, 12(3): 43−48+55.
LIU Jin, LI Jiangbo, YE Bing. Research on data security internal control risk management based on UEBA[J]. Cyberspace Security, 2021, 12(3): 43−48+55(in Chinese).

收稿日期：2022−04−19

作者简介：
马骁 (1976)，男，高级工程师，研究方向为电力二次系统安全防护等，E-mail：maxiao3@sgepri.sgcc.com.cn；
崔旭东 (1981)，男，通信作者，硕士，高级工程师，研究方向为电力二次系统安全防护、软件体系架构等，E-mail：cuixudong@sgepri.sgcc.com.cn；
李勃 (1978)，男，工程师，研究方向为计算机科学与技术等，E-mail：libo5@sgepri.sgcc.com.cn。