基于RPA技术的网络安全运营自动化实践应用研究

周映
（中国联合网络通信有限公司软件研究院，北京 100176）

摘　要：研究了围绕网络与信息系统的全生命周期，面向网络安全运营全流程场景，以机器人流程自动化（robotic process automation，RPA）技术和自适应网络安全技术建立能力框架，以期解决网络安全运营工作人工依赖性高、网络安全能力平台相对割裂、网络安全运营工作要点缺失等普适性痛点问题。构建了基于RPA技术的网络安全运营自动化平台，实现主要日常性网络安全工作的自动化转型，并将剩余人力资源配置到暂时不能自动化的领域，如业务层网络安全分析、业务网络安全渗透、漏洞挖掘、自动化运营脚本编制等方面，最终达到缓解人力不足，解决人员缺失，避免网络安全工作覆盖面不全、效能不高等目的。

关键词：机器人流程自动化；网络安全运营自动化平台；网络安全策略管理；网络安全运营体系；网络安全
中图分类号：TP391
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024190

Application research on network security operation automation practice based on RPA technology

ZHOU Ying
Software Research Institute of China United Network Co., Ltd., Beijing 100176, China

Abstract: The research focuses on the entire lifecycle of networks and information systems, aiming at the full-process scenarios of cybersecurity operations. It establishes a capability framework based on robotic process automation (RPA) technology and adaptive cybersecurity technology, along with address the common pain points in cybersecurity operations, such as high manual dependency, relatively fragmented cybersecurity capability platforms, and missing key points in cybersecurity operations. By constructing an automated cybersecurity operation platform based on RPA technology, the automation transformation of daily cybersecurity work was realized, and the remaining human resources were allocated areas that cannot be automated at the moment, such as business-level cybersecurity analysis, business network security penetration, vulnerability mining, and automated operation script development. Ultimately, it aims to alleviate the contradiction of insufficient manpower, reduce personnel shortages, and improve the coverage and efficiency of cybersecurity work.

Key words: RPA, network security operation automation platform, network security policy management, network security operation system, network security

收稿日期：2024−04−16；修回日期：2024−07−15

0　引言

日常网络安全运营工作的成效高度依赖各类运营人员的主动性和技术水平，可能存在运营效率低，流程运转缓慢，周期性网络安全检测间隔时间长，部分工作由于人手等原因无法实际执行、难以确保闭环管理等问题[1-2]，并且难以有效缩短发现风险要素和脆弱性处置时间，无法满足防守方发现及响应的时间低于攻击者发现并利用脆弱性的时间这一根本攻防原则要求[3]。

针对事件监测应急，国内网络安全行业通过安全编排、自动化和响应（security orchestration, automation and response，SOAR）技术力图优化事件处理流程，提高自动化水平[4-5]。但在包括事件监测应急在内的网络安全运营体系中，作为网络安全运营主体，占据各类人员网络安全投入时间最多的规划、开发、接入、变更、退服等日常性网络安全运营工作，以及护网、重大活动保障等工作，却缺乏强有力的技术支撑能力，依然高度依赖人员主动性、个人技能、人力资源投入，效果不佳[6-8]。在国内网络安全人员的数量和技能与网络安全需求存在巨大差距且难以在短时间内解决的情况下，主要通过改进人员这一要素解决上述问题是不可持续的。

在此背景下，研究围绕网络及信息系统生命周期，运用机器人流程自动化（robotic process automation，RPA）技术，建立一套网络安全运营自动化平台，覆盖网络安全运营全生命周期，涵盖网络安全运营涉及的各种场景。该平台可实现基于网络安全运营流程的资产、脆弱性、威胁等各类网络安全要素状态变化自动化触发逻辑驱动引擎，进而联动各底层专业网络安全能力平台，并建立基于运营场景和流程联动、底层能力调用三大核心技术的自适应网络安全能力框架。

该平台有效降低了对人员主动性及技术水平的依赖性，缩短了各网络安全运营流程闭环时间，全面提升各类网络安全运营事项的执行力度，在降低对人的依赖性、减少人工投入的同时，全面提升整体网络安全防护水平。

1　基于RPA技术的网络安全运营自动化平台框架

基于RPA技术，本文梳理并建立驱动平台自动化运营的60余个流程联动触发场景体系和全新的智能引擎，实现网络安全运营全场景刻画，消除传统运营高度依赖人的技能、积极性的重大缺陷，各网络安全运营场景相互关联，自动触发，最大限度保障网络安全运营工作效率[9-11]。

为了有效解决各网络安全能力平台难以应用、能力割裂、无法有效协同的问题，研究建立了基于场景的全面自适应能力框架，如图1所示。该框架为各类网络安全人员、维护人员、规划人员、管理人员提供管理责任技术支撑一站式入口。

1.1　展示层

RPA技术的工作原理为通过用户界面层操作，模拟人类在计算机上执行的各种任务。由于RPA技术是在用户界面层进行操作的，因此它不需要对现有系统进行大规模的修改或替换，这使得RPA技术的实施变得相对简单和快捷。展示层是RPA平台的前端页面展示，包括系统管理、运营入口及指标展示3部分。

- 系统管理可实现对整个网络安全运营自动化平台的参数配置，包括用户管理、流程配置、接口配置等功能。
- 运营入口为各专业人员的访问入口，根据职责不同，划分对应运营场景相关权限。如基础设施运维人员可基于该入口执行资产变更管理、脆弱性全生命周期管理、网络安全策略管理、账号口令管

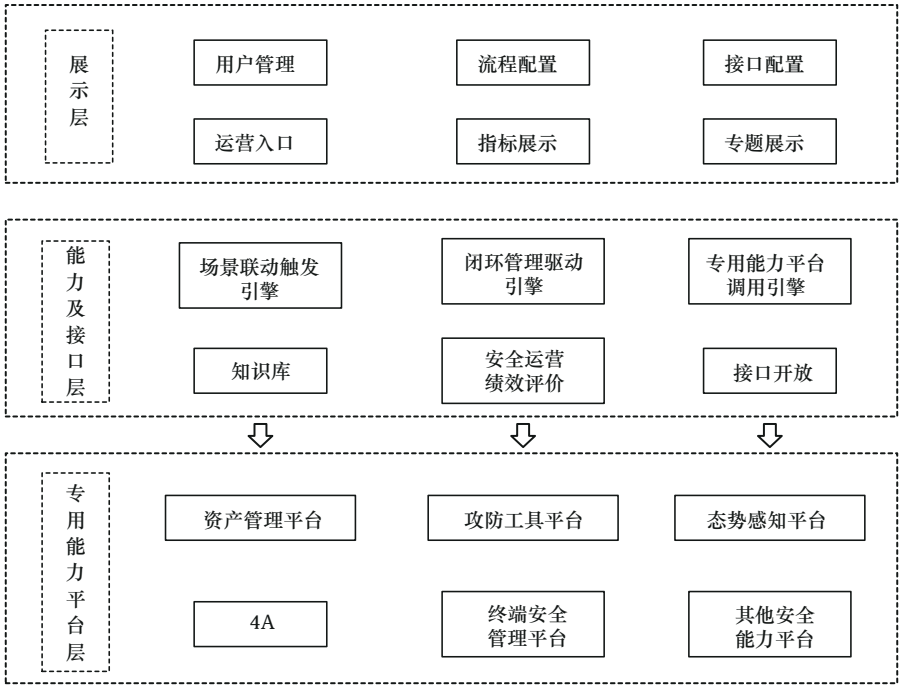

图1　基于场景的全面自适应能力框架

理等流程，网络安全测试人员可访问系统网络安全准入测试流程、漏洞管理流程等。同时，运营入口提供根据重大活动保障关注的系统范围、网络安全管理侧重点，选择、组合并构建专用展示窗口的能力，在活动结束、数据备份之后释放资源，为低成本、高效率开展重大活动提供了一个崭新思路。

- 指标展示是对整体网络安全运营相关指标的统一展示，包含常态化运营指标及专题指标展示。专题指标展示，根据专题不同重点突出关键指标，如攻防演练重点展示网络安全预警管理流程、网络安全事件管理流程等。

1.2　能力及接口层

能力及接口层主要包括基于网络安全要素状态变化基础上的60余个场景联动触发引擎、10余个专用能力平台调用引擎、闭环管理驱动引擎等功能。

场景联动触发引擎，负责按照流程场景关联关系，根据流程中任务节点的处理结果，即网络安全要素变化，进行自动判断，确定是否触发关联流程（后序流程），并对触发的关联流程自动携带流程输入信息，跟踪执行情况，完成整体流程活动。使用RPA工具提供的可视化编辑器，将业务流程拆分成多个任务节点，并定义它们之间的逻辑关系。该功能为每个任务节点配置具体的操作，如数据输入、表单提交、系统调用等，定义流程启动的条件，以及任务节点之间的触发条件，在模拟环境中测试编辑好的流程，根据测试结果进行优化和调整。

闭环管理驱动引擎，主要用于对网络安全运营流程进行督促闭环，针对处理缓慢或超时的任务节点，自动进行提醒和告警，包括电子邮件、短消息等方式。资产变更管理流程如图2所示。引擎会实时监控RPA流程中每个任务节点的执行状态和处理时间。如果某个任务节点的处理时间超过预设的阈值，引擎会判定其超时。对于超时的任务节点，引擎会自动发送告警信息给相关人员，提醒他们进行处理，并跟踪告警信息的处理

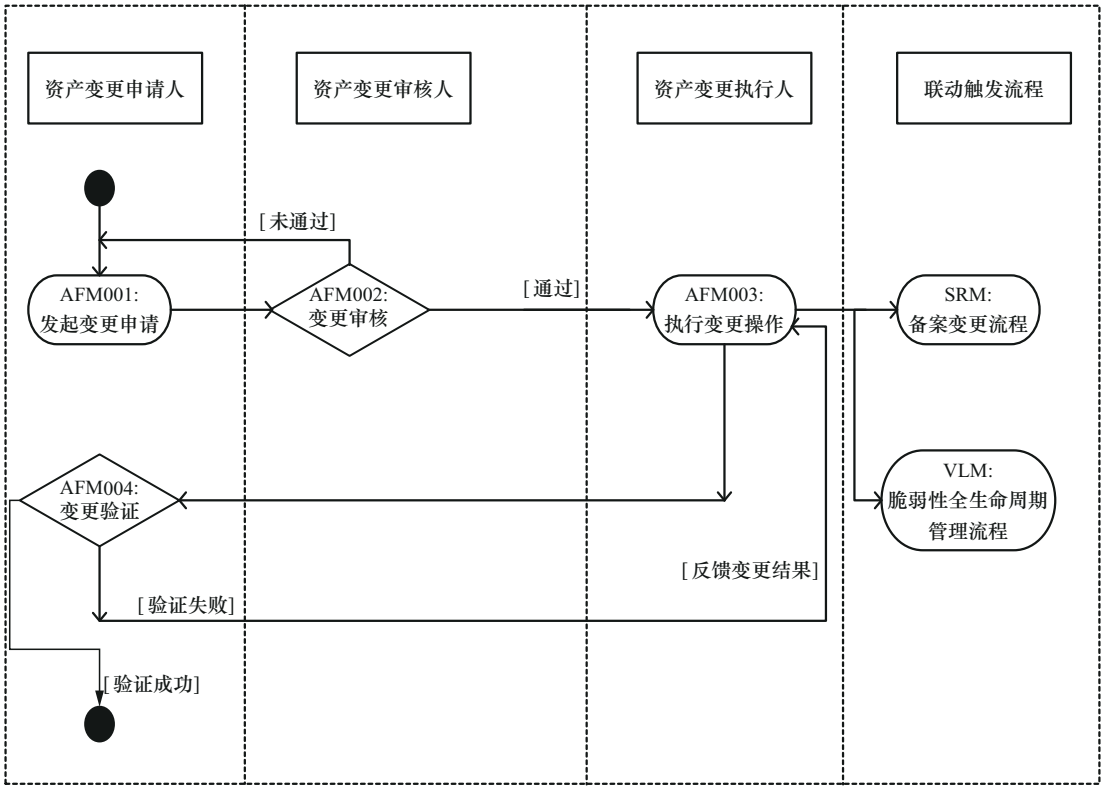

图2　资产变更管理流程

结果，确保问题得到及时解决。当出现资产变更时，变更执行成功后，自动触发定级备案变更流程、基线管理流程、漏洞管理流程等，将传统的由网络安全人员或者系统管理人员根据维护作业计划定期执行网络安全检测的模式改变为由平台即时启动对应检测任务的新模式，从而将问题发现、驱动处置的时长从传统的数小时甚至数周缩短为即时完成，实现革命性变化。

专用能力平台调用引擎，负责对流程中需要调用底层网络安全平台能力的场景，自动调用相关接口，获取网络安全要素数据、下发处置任务，完成相关动作。

1.3　专用能力平台层

专用能力平台层主要包括已有的资产管理平台、虚拟专用网络（virtual private network，VPN）、4A（认证、授权、账号、审计（authentication, authorization, account, audit））、攻防工具平台、脆弱性管理、基线合规等网络安全能力，处理接收各类网络安全运营任务，提供基础能力支撑。以攻防工具平台为例，该平台提供代码审计、漏洞扫描等功能，支撑网络安全开发管理流程、漏洞管理流程。

研究涉及的网络安全运营自动化平台主要包括展示层、能力及接口层，专用能力平台仅配合项目实现自动化平台驱动的调用功能。

研究建设的网络安全运营自动化平台围绕系统全生命周期，覆盖系统规划、建设、上线、运营、退服各个阶段，建立了完善的网络安全运营流程体系，包含网络安全规划流程、网络安全准入测试流程、网络安全事件管理流程等30余个流程[12-15]，安全运营流程体系见表1。

研究在平台中实现了上述运营流程，以及各个流程中基于资产、脆弱性、威胁在内的安全要素状态变化设计的60余个自动化流程联动触发逻辑（见表2）引擎。在平台构建中，使用RPA工具中的接口调用功能，与专用能力平台的应用程

表1 安全运营流程体系

序号	流程名称	序号	流程名称	序号	流程名称
1	信息安全管理体系全生命周期管理	12	网络安全事件管理	23	敏感数据访问授权
2	等级保护管理	13	网络安全监控	24	密钥管理
3	网络安全审查管理	14	网络安全域管理	25	网络安全策略管理
4	系统网络安全规划	15	网络安全配置管理	26	网络安全开发管理
5	网络安全工程建设	16	补丁管理	27	终端接入管理
6	系统网络安全准入测试	17	防病毒管理	28	资产变更管理
7	风险评估管理	18	系统互联管理	29	脆弱性全生命周期管理
8	数据备份管理	19	远程接入管理	30	网络安全平台资产接入与退出
9	软件变更管理	20	账号口令管理	31	安全审计管理
10	业务连续性管理	21	网络安全应急预案管理	32	日常维护作业计划管理
11	网络安全预警管理	22	物理访问控制管理	33	网络安全退服管理

序接口进行对接，实现数据的双向传输和指令发送。对接完成后，进行接口验证和测试，确保数据的准确性和指令的有效性。使用RPA工具中的流程建模功能，根据表1中的网络安全运营流程体系，构建相应的业务流程模型。为每个流程模型配置具体的任务节点，包括从专用能力平台获取数据、执行特定操作、发送告警等。根据业务需求和安全要素状态变化，设置任务节点的触发条件，如定时触发、事件触发等。通过RPA工具的自动化执行引擎，按照预定的逻辑和触发条件，自动执行流程中的任务节点。使用RPA工具或专用能力平台提供的功能，实时监控资产、脆弱性、威胁等安全要素的状态变化。根据表2中的自动化流程联动触发逻辑，设计相应的触发规则和逻辑。当安全要素状态发生变化时，根据预设的触发逻辑，自动触发相应的流程或任务节点。在RPA工具中建立问题管理系统，记录每个问题的详细信息，包括问题描述、处理状态、责任人等。通过RPA工具的自动化执行和监控功能，实时跟踪问题的处理进度和结果。对于未处理或处理超时的问题，通过电子邮件、短消息等方式自动发送告警信息给相关人员，确保问题得到及时解决。

此外，研究结合自动化问题管理闭环跟踪机制，实现以平台自动化执行周期性监测、网络安全要素状态变化实时自动化触发联动处置活动及闭环跟踪、重大活动保障场景快速设定等能力构成的自动化运营系统。

2 网络安全策略管理流程触发逻辑规则示例

在风险评估、安全审计、发现安全预警时，需要调整访问控制网络安全策略以消除网络安全风险。此外，网络安全监控发现网络安全事件后，需要调整网络安全策略以拦截攻击、加固防护对象时，也需要及时触发网络安全策略管理流程，消除安全风险。

在设备退服阶段，除设备下线以外，该设备部署的网络边界访问控制设备，如防火墙、路由器、交换机中对应的访问控制策略均需要关闭原有的开放访问策略。与该设备存在互联关系的对端系统，同样也需要关闭原来授权的访问控制策略，一方面，是为了减少垃圾策略以提升网络访

表2　基于网络安全要素状态变化设计的自动化流程联动触发逻辑

阶段	前序流程名称	后续流程名称	联动时间间隔
网络系统安全规划	信息安全管理体系全生命周期管理流程	无	—
	系统网络安全规划流程	入网网络安全测试管理	不确定
		网络安全工程建设流程	不确定
网络安全开发	网络安全开发管理流程	无	
系统安全建设	SPCM 网络安全工程建设流程	入网网络安全测试管理	即时
		网络安全平台接入与退出	即时
		网络安全应急预案管理流程	即时
		系统互联管理流程	即时
		网络安全域管理	即时
		账号口令管理	
		网络安全策略管理流程	即时
	等级保护管理流程	无	—
	安全审查管理流程	无	—
	入网安全测试管理流程	网络安全开发管理流程	即时

问控制设备的处理性能；另一方面，可避免相关策略被滥用，进行网络安全攻击。研究设计的联动触发场景见表3。

研究设计的触发逻辑流程主要涉及3种动作，分别为策略开通、策略调整、策略关闭。

此外，在研究的参数传递规则中，前序流程需要向本流程传递的参数至少包括：触发联动调用动作类型，如开通或者关闭，需要提供策略设置所需要的五元组以及两端系统名称、设备名称，如变更，需要提供策略变更所需要的五元组以及两端系统名称、设备名称以及之前策略开通时提供的五元组；联动需求说明等。

最后，联动触发返回结果，按照调用动作类型，分别返回策略开通、调整、关闭完成与否的结果。

在网络安全能力自动调用中，研究针对已有的10余种网络安全能力，如VPN、4A、网页应用防火墙（web application firewall，WAF）、漏扫平台等能力，基于接口调用的方式，根据网络安全运营需要，按场景编排模板自动采集网络安全要素状态变化数据、下发任务指令，建立自适应网络安全能力框架，提升网络安全运营质效。

研究设计的网络安全运营自动化平台对各网络安全运营流程绩效指标进行实时展示。针对常态化运营、重大活动保障、攻防演习等特定场景，差异化专题展示，突出重点指标，及时发现网络安全运营风险点，动态调整，及时采取措施规避，促进网络安全运营体系不断完善。

3　RPA技术与传统自动化技术对比

RPA技术与传统自动化技术相比，RPA技术具有较高的自动化程度，能够实现全流程的自动

表3　联动触发场景

前序流程名称	触发后序流程的条件	后序流程名称	联动时间间隔
网络安全工程建设	设备部署、网络连接	网络安全策略管理	即时
风险评估管理	评估发现访问控制策略过宽等风险	网络安全策略管理	即时
网络安全审计	发现访问控制策略管理规定及执行缺陷	网络安全策略管理	即时
网络安全预警	有需要调整网络安全策略的网络安全预警	网络安全策略管理	即时
网络安全监控	发现利用了网络安全策略缺陷的网络安全事件	网络安全策略管理	即时

化，通过模拟人工操作，控制各种应用软件和浏览器，并可跨系统处理信息，且其脚本编制简单，业务人员容易学习和修正。而传统自动化技术的自动化程度较低，通常只能实现部分自动化，需要人工进行任务流转或系统操作，脚本编制复杂，需要专业技术人员完成且难以修改。其次，RPA技术在实施效果上表现出显著的效率提升，能大幅减少人力成本，在处理大量、重复性工作时效果尤为突出，且能够降低错误率，提高业务处理的准确性和可靠性。此外，RPA技术的灵活性强，能够快速适应业务变化，通过调整脚本或规则迅速应对新需求。相比之下，传统自动化技术在提高效率和降低错误率方面效果不如RPA显著，且灵活性较差，需要通过较大改动和调整来应对业务变化。最后，在应用场景方面，RPA技术适用范围广泛，可应用于各种需要大量、重复性操作的业务流程，在金融、制造、电商、电信等多个行业都有广泛应用，而传统自动化技术适用场景和行业相对有限，通常只能应用于特定系统或领域。

可编程逻辑控制器（programmable logic controller，PLC）是一种集成了计算机、通信和自动控制技术的工业控制装置。它采用大规模集成电路技术，具备抗干扰技术，可减少继电器系统中的机械触点和复杂接线，提高系统的可靠性和平均无故障时间。当PLC运行时，中央处理器（central processing unit，CPU）根据用户按控制要求编制好并存于用户存储器中的程序，按指令步骤号（或地址号）作周期性循环扫描。这个过程可分为输入采样、用户程序执行和输出刷新3个阶段。在输入采样阶段，PLC以扫描方式依次读入所有输入状态和数据，将它们存入计算机接口（input/output，I/O）映像区中的相应单元内，并进入用户程序执行阶段，按由上而下的顺序依次扫描用户程序（梯形图）。在扫描每一条梯形图时，先扫描梯形图左边由各触点构成的控制线路，进行逻辑运算，然后根据逻辑运算的结果刷新输出状态。最后，在输出刷新阶段，CPU按照I/O映象区内对应的状态和数据刷新所有的输出锁存电路，再经输出电路驱动相应的外设。将PLC和RPA技术进行对比，RPA技术能够模拟人工操作，控制各种应用软件和浏览器，实现业务流程的全流程自动化，无须人工干预。

RPA技术作为传统平台开发方式的一种有效补充，可以嵌入如业务流程管理（business process management，BPM）系统等传统系统软件中以完成部门的、专业的重复性工作，也可以运行在更高的软件层级，直接连接顶层软件。它不会对已有软件系统进行侵入影响，在协助企业提升效能过程中，保障企业已有系统功能平稳、可靠运行。

4 RPA驱动的网络安全运营自动化实践案例

4.1 RPA驱动的网络安全运营自动化应用实践

4.1.1 某电信企业的RPA应用

以某电信企业为例，该企业在网络安全运营中需要人工监控和分析海量日志数据，遇到突发安全事件时，人工处理难以迅速隔离和解决问题；系统补丁管理依赖手动扫描安装，容易遗漏关键更新。为了解决这些问题，该企业引入RPA技术，通过需求分析确立了3项自动化流程：日志监控与分析、事件响应与处理、补丁更新管理。日志监控流程定期从各系统拉取日志，利用机器学习算法分析日志内容，识别异常行为并生成报告，为运营团队提供有力支持。

为RPA自动化平台设计了直观易用的前端页面，由系统管理、运营入口和指标展示3个主要部分组成，如图3所示。

系统管理部分允许管理员配置平台参数，如运营入口为不同职责的专业人员提供了定制化的访问权限，确保他们只能访问和执行与其职责相

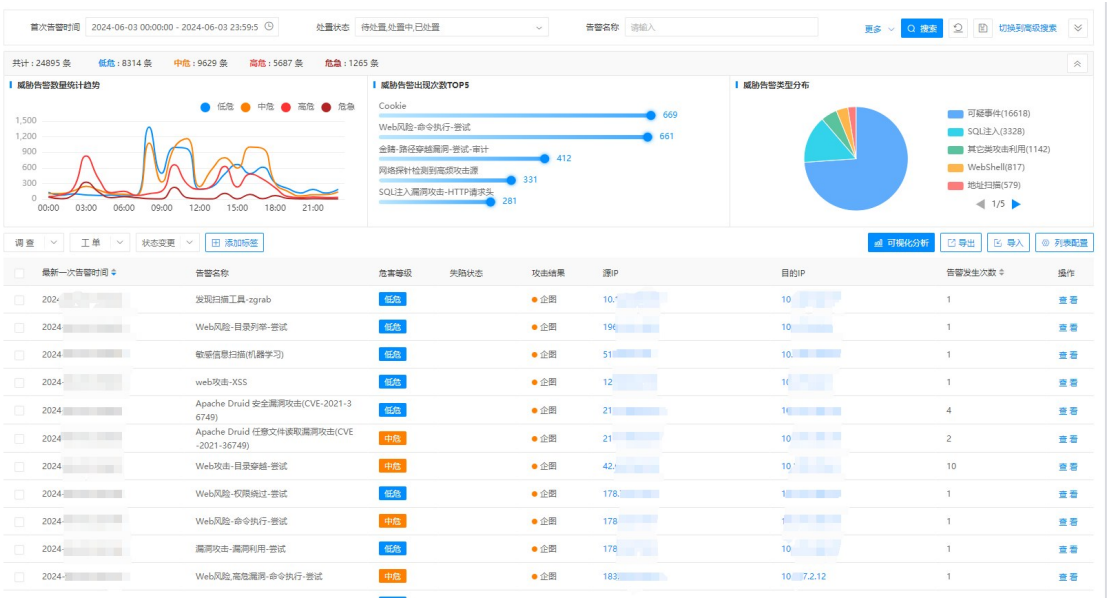

图3　某电信公司的RPA平台前端页面

关的任务。指标展示部分则提供了全面的网络安全运营指标数据，帮助管理层和决策者快速了解系统安全状况。

在能力及接口层，电信公司开发了流程编辑、场景联动触发引擎、闭环管理驱动引擎等功能模块。流程编辑功能允许管理员根据业务需求自定义工作流程；场景联动触发引擎能够根据网络安全要素状态变化自动触发关联流程；闭环管理驱动引擎则确保所有任务都能得到及时闭环处理。此外，公司还开发了专用平台能力调用引擎，用于调用底层网络安全平台的能力。

在系统设计与开发完成后，电信公司组织了针对RPA技术和网络安全运营自动化平台的员工培训。培训内容涵盖了RPA技术原理、系统操作流程、故障排查与解决等方面，如图4所示。同时，公司还进行了上线测试，确保系统能够稳定运行并满足业务需求。在测试过程中，员工积极参与并反馈了宝贵的意见和建议，帮助公司不断优化和完善系统。

经过充分的测试和调整，电信公司的网络安全运营自动化平台正式上线，公司还定期对系统进行优化和升级，以适应不断变化的网络安全环境和业务需求。此外，公司还积极收集用户的反馈和建议，不断完善系统的功能和性能以满足用户的实际需求。

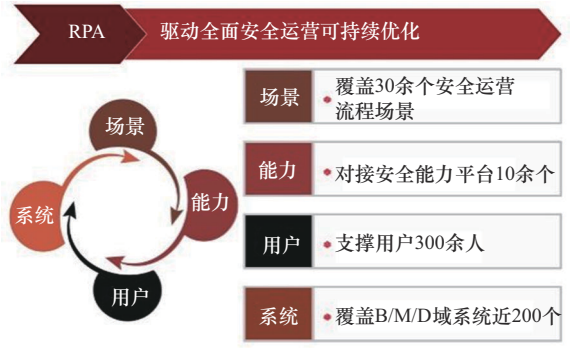

图4　公司人员参与针对RPA技术和网络安全运营自动化平台的培训

4.1.2　某金融企业的RPA应用

某金融企业的VPN系统因为安全性要求设置了90天未使用账号自动锁定的安全策略，但VPN系统未提供自动解锁功能，因此账号解锁一直采用用户电话申告管理员的方式，必须由系统管理员人工进行自动解锁功能，耗费了维护人员大量的精力。VPN系统属于硬件类产品且属于厂商提供的一体化的标准产品，原厂通常不愿意进行定制化改造。因此，该企业引入了RPA机器

人，由用户自主申请解锁登记，RPA机器人代替维护人员检查申请信息，自动进行账户解锁并及时通知用户解锁。

经过市场调研和需求分析，企业选择了具备高度可定制性和可扩展性的RPA解决方案，确保能够满足网络安全运营的复杂需求，并对现有的安全管理系统、安全信息和事件管理（security information and event management，SIEM）平台等进行集成，确保RPA解决方案能够无缝对接，实现数据共享和流程协同[16]。为提高企业人员对RPA技术的应用熟练度，企业通过案例分析和模拟操作，让学员熟悉RPA解决方案在网络安全运营中的实际应用。培训周期为一个月，分为理论学习和实践操作两个阶段，各两周时间，采用线上、线下相结合的培训形式，线上通过视频会议进行理论授课，线下组织学员到实际环境中进行实践操作。

经过RPA技术的引入和应用，网络安全运营的自动化程度得到了显著提升，原本需要人工处理的大量重复性工作，现在可以通过RPA机器人自动完成，极大地提高了工作效率。

4.2 RPA驱动的网络安全运营自动化实践成果

4.2.1 某电信企业的RPA应用成效

引入RPA之前，该电信公司对于日志的处理每天需要投入3名员工，每人工作8 h，共计24 h/天，其误报率约为15%，漏报率约为5%。对于安全事件，需要5名员工，每人工作8 h，共计40 h/天。人为判断容易导致响应不及时，响应及时率仅为80%。补丁更新的管理需要2名员工，每人工作8 h，共计16 h/天。人为操作易出现遗漏，补丁更新遗漏率约为10%。处理VPN账号锁定状态需要1名员工，每人工作8 h，共计8 h/天。人为处理容易出现疏漏，解锁成功率仅为95%。引入RPA技术后，RPA系统自动完成日志监控分析，用时缩短至1 h，相当于1 h/天，误报率降低至5%，漏报率降低至2%。RPA系统还自动识别和分类网络安全事件，用时缩短至1.8 h，相当于2 h/天，响应及时率提升至95%。同时，自动检测和更新终端设备的补丁，用时缩短至3.5 h，相当于4.2 h/天，补丁更新遗漏率降低至5%。对于VPN账号自动解锁，RPA系统自动检测和处理VPN账号的锁定状态，用时缩短至20 min，相当于0.33 h/天，解锁成功率提升至99%。

企业在应用RPA技术后，整体运营效率提升约25%，工作准确性提高，误报率和漏报率显著降低，网络安全防护能力提升，补丁更新遗漏率降低，解锁成功率提升。

4.2.2 某金融企业的RPA应用成效

在引入RPA机器人之前，某金融企业的VPN账号解锁流程相当烦琐，且效率低下。该企业每天大约有50个用户需要解锁账号，而每个解锁请求平均需要管理员花费15 min来处理，这意味着管理员每天大约有750 min，即12.5 h被用于处理这一重复性的工作，而每周总时间将高达87.5 h，占总运维时间的近40%。

引入RPA机器人后，每个解锁请求的处理时间从15 min降低到5 min，每天可以节省约8.3 h的人工操作时间，每周可以节省约58 h，占总运维时间的近30%。同时，RPA机器人解锁成功率达到99.9%，远高于人工解锁的90%，说明其提高了运维效率，改进了用户体验。引入RPA机器人后，该企业的运维效率得到了显著提升。以前，管理员需要花费大量时间处理的重复性工作，现在可以由RPA机器人自动完成，释放了管理员的时间，使他们能够更多地关注其他重要的运维工作。由于RPA机器人可以快速部署，无须进行复杂的系统定制，因此节约了大量的开发和维护成本。

5 结束语

本文设计了一套网络安全运营自动化平台，提升了网络安全运营自动化程度，通过自动化调

用、充分发挥下游各网络安全能力平台效能，支撑围绕风险管理各要素状态变化、各网络安全能力自动化协同联动的网络安全运营工作高速、流畅运转。基于此目标，主要任务分为网络安全运营流程体系建设、RPA 驱动的网络安全运营自动化平台建设、与底层网络安全能力联动调用对接等方面，并全面支撑日常网络安全运维、重大活动保障和网络安全运营工作完全可视化。

本文通过使用网络安全运营自动化平台，解决了网络安全运营人员工作量大、跨部门专业沟通成本高、技术水平依赖性强的问题。基于 RPA 技术理念，自适应网络安全能力框架，总体上明确了各类能力平台和网络安全设备以及网络与系统内生网络安全之间的逻辑关系和协同机制，有效降低了人工成本，提升了网络安全运营效率。

未来将着重研究提升网络安全运营自动化平台的智能化与自主决策能力，结合人工智能和机器学习技术实现自适应学习和实时威胁响应；探索多层次协同防御机制，跨越应用层、安全层和物理层；推动安全运营数据的可视化与实时分析，增强态势感知和决策支持，实现自动化能力的标准化。

参考文献：

[1] 冯文芳, 田文中, 杨雯琪. 基于微服务与中台理念的财务共享管理平台设计[J]. 财会通讯, 2022(6): 167-171.
FENG W F, TIAN W Z, YANG W Q. Design of financial sharing management platform based on micro-service and middle platform concept[J]. Communication of Finance and Accounting, 2022(6): 167-171.

[2] 张杨军, 闫宇洁, 孙敏. “大智移云” 背景下的 RPA 在财务共享中的应用[J]. 财会学习, 2022(6): 44-46.
ZHANG Y J, YAN Y J, SUN M. Application of RPA in financial sharing under the background of“great wisdom moves to the cloud”[J]. Accounting Learning, 2022(6): 44-46.

[3] 孙逸, 董志强. RPA: 财务智能化的必经之路[J]. 新理财, 2017(11): 64-65.
SUN Y, DONG Z Q. RPA: the only way for financial intelligence[J]. Corporate Finance, 2017(11): 64-65.

[4] 汪涛, 吴耿锋, 黄力芹. 工作流管理的现状和未来趋势[J]. 小型微型计算机系统, 2001, 22(2): 232-236.
WANG T, WU G F, HUANG L Q. Status quo and the future of workflow management[J]. Mini-micro Systems, 2001, 22(2): 232-236.

[5] 马莉娟, 沈娜娜, 陈刚. RPA 在电网行业财务领域的应用探索[J]. 科技与创新, 2018(22): 16-20.
MA L J, SHEN N N, CHEN G. Application of RPA in the financial field of power grid industry[J]. Science and Technology & Innovation, 2018(22): 16-20.

[6] 王言. RPA: 流程自动化引领数字劳动力革命[M]. 北京: 机械工业出版社, 2020.
WANG Y. RPA: process automation leads the digital labor revolution[M]. Beijing: Machinery Industry Press, 2020.

[7] 彭伟锋, 吕易立, 刘振辉. 供电企业营销领域 RPA 技术的研究与应用[J]. 中国新通信, 2020, 22(19): 120-121.
PENG W F, LYU Y L, LIU Z H. Research and application of RPA technology in marketing field of power supply enterprises[J]. China New Telecommunications, 2020, 22(19): 120-121.

[8] 欧阳昱, 张衡, 孙琼, 等. 电网企业基于 RPA 技术的营配调贯通数字员工研究应用[J]. 电气传动自动化, 2020, 42(6): 31-33.
OUYANG Y, ZHANG H, SUN Q, et al. Research and application of digital staff in operation, distribution and adjustment of power grid enterprises based on RPA technology[J]. Electric Drive Automation, 2020, 42(6): 31-33.

[9] 陈春丽. 基于 RPA 的财务智能化与业务协同创新研究[J]. 办公自动化, 2024, 29(6): 93-96.
CHEN C L. Research on the financial intellectualization and business collaborative innovation based on RPA[J]. Office Informatization, 2024, 29(6): 93-96.

[10] 谢紫微. 数字化转型背景下 RPA 在财务共享服务中心的应用: 以费用业务为例[J]. 中小企业管理与科技, 2024(1): 139-141.
XIE Z W. Application of RPA in financial shared service center under the background of digital transformation—taking expense business as an example[J]. Management & Technology of SME, 2024(1): 139-141.

[11] 傅昊. 深化数字化转型 103 个 RPA 场景上线[J]. 华北电业, 2023(12): 68-69.
FU H. Deepen the digital transformation, 103 RPA scenes are launched[J]. North China Power, 2023(12): 68-69.

[12] 祃安源, 吕思潼. RPA 深化应用提升工作效率[J]. 中国电力企业管理, 2023(29): 81.
MA A Y, LYU S T. RPA deepens application and improves work efficiency[J]. China Power Enterprise Management, 2023

(29): 81.

[13] 郭丽娟. RPA技术在财务共享业务流程优化中的应用探究[J]. 中国管理信息化, 2023, 26(20): 67-69.
GUO L J. Research on the application of RPA technology in financial sharing business process optimization[J]. China Management Informationization, 2023, 26(20): 67-69.

[14] 赖琪, 蔡宇辉, 夏斯琼, 等. RPA流程标准化定义与设计[J]. 计算机科学, 2023, 50(12): 82-88.
LAI Q, CAI Y H, XIA S Q, et al. Standardization definition and design of robotic process automation[J]. Computer Science, 2023, 50(12): 82-88.

[15] 谭永丽. 基于RPA的H公司数据报送流程优化研究[D]. 大连: 大连海事大学, 2023.
TAN Y L. Research on optimization of data submission process of H company based on RPA[D]. Dalian: Dalian Maritime University, 2023.

[16] 许广繁, 柏建宁. 基于RPA金融业务运营的应用研究[J]. 中国管理信息化, 2022, 25(13): 74-77.
XU G F, BAI J N. Research on the application of financial business operation based on RPA[J]. China Management Informationization, 2022, 25(13): 74-77.

[作者简介]

周映（1983− ），女，中国联合网络通信有限公司软件研究院副总架构师、高级工程师，主要研究方向为网络与信息安全防护体系搭建及攻防技术、网络与信息安全运营体系、安全事件应急响应及数据安全管理体系搭建等。