 DOI: https://doi.org/10.12349/iser.v5i6.2964

Reflection on the Integration Construction of Network Security and Information Operation and Maintenance

Yanfeng Liu

Sinopec East China Oil and Gas Branch, Nanjing, Jiangsu, 210019, China

Abstract

This paper discusses the necessity and practice of establishing an integrated platform of network security and information operation and maintenance. Through the integration of security and operation and maintenance technology forces, realize the efficient sharing of resources and information, and improve the overall operation and maintenance efficiency and security level. Put forward the construction plan of the integrated platform of network security and information technology, through the integration of the platform, realize resource and information sharing, network security and operation and maintenance integration operation, focus on the work perspective, aggregate technical capabilities, centralized monitoring and management, realize the improvement of enterprise network security management ability, and the optimization of operation and maintenance management process. Looking ahead, we will further use artificial intelligence and automation technology to promote the development of operation, peacekeeping and security management to a more efficient and intelligent direction.

Keywords

network security; information operation and maintenance; integrated platform

网络安全与信息化运维一体化建设思考

刘砚峰

中国石化华东油气分公司，中国 · 江苏 南京 210019

摘　要

论文探讨了建立网络安全与信息化运维一体化平台的必要性与实践。讨论通过整合安全与运维技术力量，实现资源和信息的高效共享，提升整体的运维效率和安全水平。提出网络安全与信息化一体化平台的建设方案，通过平台整合集成，实现资源和信息共享，网络安全与运维一体化运行，聚焦工作视角，聚合技术能力，集中监控和管理，实现企业网络安全管理能力提升，运维管理流程优化。展望未来，进一步利用人工智能和自动化技术推动运维和安全管理向更高效、更智能的方向发展。

关键词

网络安全；信息化运维；一体化平台

1 概述

随着互联网、大数据、云计算、人工智能等技术的加速发展，数字化转型工作的快速推进对网络安全工作和信息化运维工作提出了更高的要求 [1]，建设全新的网络安全与运维一体化工作体系，保障整体架构的安全、稳定运行是信息化发展的迫切需求。

信息化运行管理过程中，网络安全与信息系统运维是相辅相成的两个方面，它们共同确保了整个 IT 基础设施的稳定、安全和高效运行。运维负责信息系统的稳定运行和性能最优，网络安全则关注保护系统免受各种威胁和攻击，如病毒、黑客攻击、数据泄露。有效的安全防护措施，可以防止未经授权的访问和防范网络威胁，确保信息系统的平稳运行，安全的信息化运行环境是保证信息系统的完整性和可用性的基础。可以说，在日常 IT 运营管理中，网络安全与信息系统运维工作密切相关。但是实际运营中，很多企业会分别组建独立运维团队和安全团队，独立运作，实际形成一种较为割裂的局面，带来一系列问题。

举个例子，如果一台服务器因攻击宕机了，需要恢复、需要解决风险或隐患。它既是运维工作，也是安全工作，如果运维与安全工作分开独立运行，会形成一种博弈的局面。因为运维需要的是效率，而安全需要的是周全。特别是在运行考核不断严格的条件下，将优先考虑系统恢复运行，而溯源、加固等安全工作得不到充分重视，导致信息系统长期带病运行。

整合安全和运维技术力量，实现资源和信息共享，是比较合理的发展方向。技术力量整合的前提是工作界面的统

【作者简介】刘砚峰（1976–），男，中国江苏南京人，硕士，高级工程师，从事网络安全与信息系统运维研究。

一，建设一体化的安全运维平台，将网络安全与运维工作集中到一个平台运行，有助于聚焦管控视角，聚合技术力量，促进信息化运维与网络安全防护工作相对最优化运行。

2 面临的挑战和解决方案

由于建设时期和重视程度的差异，企业通常首先建立信息化运维平台，随后再开发网络安全管控平台。这两个平台在建设目标和发展方向上相对独立，客观上导致了运维管理与网络安全防护之间的割裂。下面具体分析这种现象带来的挑战，并探讨解决方案。

2.1 信息化运维工作的挑战

从信息化整体视角看，运维工作面在不断地拓展。一是随着云计算、大数据、虚拟化、容器化技术的发展，后端服务器、系统架构越来越复杂；二是伴随 5G 和物联网技术的发展，网络不断扩展至生产车间和现场，尤其是在工业制造企业中，企业网络已广泛覆盖生产现场；三是信创（信息化创新）工作的快速推进，带来了前后端软硬件体系架构的重大变革。

2.2 网络安全运维工作的挑战

从网络安全的视角看，安全防护的范围和难度也在不断增加。一是随着国际形势的变化，网络安全形势更加严峻，外部威胁出现新变化，APT、供应链攻击更加频繁且破坏力更强；二是随着网络的延伸，生产现场网络逐渐暴露，工控系统面临巨大威胁，三是信息化体系架构趋于复杂，对网络安全人员的技术能力提出了更高的要求。

2.3 共同挑战

同时，运维还是网络安全工作还面临着一个共同的挑战：由于软硬件设备、监控防护设备数量众多，种类多样，各类运行数据、日志、报警信息分散，视角不聚焦，技术人员很难全面掌握整体运行、安全态势。大部分时间用于处理随时出现的问题，工作被动、低效。

2.4 解决方案

2.4.1 安全运维一体化（SecOps）

安全运维（SecOps）理论，提出将安全措施和流程集成到信息系统运维中的方法。组建安全运维团队，通过自动化工具和持续的合作流程及时识别修复安全问题，同时不会显著影响系统性能。具体实施方法包括，部署安全信息和事件管理（SIEM）系统，自动化响应系统等工具，开展持续监控，实时监控网络和系统活动，及时检测异常行为或事件，设计协作流程，确保信息共享和沟通畅通，让安全和运维能够协同高效工作。

2.4.2 ITIL V4

2019 年发布的 ITIL Foundation V4 版本中，提出了将安全性集成到服务管理过程中提出了更新和改进的方法，引入服务价值系统（Service Value System，SVS），强调了通过各种管理能力和组件，在企业中创建、交付和持续改进服务。在 ITIL V4 中，网络安全不再在单一节点或过程中的考虑，而是成为贯穿整个服务的每个活动和实践的基本组成部分。这将提高安全防护的适应性和实时响应能力。

3 建设方案

3.1 总体思路

考虑到在运维与安全防护方面的前期建设，安全运维一体化平台的建设应尽可能通过系统集成整合的方式实现，打通与其他设备或系统，实现数据、报警信息的汇聚。既可有效降低建设成本，又可降低实施难度。同时，在平台底层引进流程引擎工具，修订或覆盖原有系统流程，实现业务全覆盖。

因此，建设总体思路是通过系统整合，打通下层异构系统，收集汇总告警、异常事件，集中监控；将运维及安全管理的工作放在一个界面运行。集成流程引擎，运用流程编排能力持续优化，实现安全管理与运维流程集成运行，闭环管理。

3.2 业务架构

在业务架构上，将系统分为三层：

数据融合层：打通异构、整体纳管安全运维工具，解决数据分散问题，构建 IT 安全运维基础能力基础库，实现异构设备、系统的统一管理、统一调度、统一运维。

业务分拨层：构建 IT 运维、网络安全一体化的业务支撑流程，实现“横向到边、纵向到底”的跨部门、跨层级的协同联动的管理模式，实现 IT 运维支撑业务提质增效。

指挥调度层：通过转变管理方式、实现 IT 运行全面监测、统一指挥、综合分析，综合运维规范化、智慧化管理目标，为决策层提供辅助决策和命令指挥，提升信息化运行质量。

根据业务架构将平台分为 5 个模块：安全运维资源库、能力纳管模块、业务流程分拨模块、安全运维应用中心和门户展示模块。

3.3 安全运维资源库

安全运维资源库是用户、资产、日志、报警等数据的集中存储中心，主要包括以下内容。

3.3.1 数字资产子库

从各类下联系统、设备收集资产数据，经汇总、清洗，形成标准化的资产信息。重点解决资产数据不全面，不准确的问题。

3.3.2 漏洞隐患信息

收储各类下联系统（如漏扫系统、服务器防护系统等）和外部公开的漏洞信息，关联资产数据，形成信息化资产的隐患治理台账。

3.3.3 威胁信息

收集各类安全防护设备的攻击、异常流量等报警，利用大数据处理能力，自动关联分析、合并验证，形成统一的

安全事件库，为网络安全事件闭环处置提供数据基础。

3.3.4 运维管理数据

收储综合运维相关数据，收集机房、网络、服务器、基础软件、日常巡检、系统定期报告等数据。

3.3.5 知识库

主要储存以下数据：

①安全与运维相关政策法规，技术标准，制度流程体系文件。

②解决方案：历史事件、故障解决方法，排除步骤等。

③上线及变更记录：已实施的上线及变更内容，经验教训等。

④培训材料和用户手册，常见问题等。

3.4 能力纳管模块

收集各类日志数据，通过 flink 计算，处理和分析不同来源的数据流，形成有价值的数据集合，分类推送至安全运维资源库。对外提供一系列标准接口，对接各类下联系统，形成统一纳管。

3.5 安全运维应用中心

为业务集成分拨模块提供对应操作界面，实现人机交互，对各类应用数据的操作能力。

3.5.1 资产管理子应用

针对数字资产子库数据，定制操作界面，包括资产信息更新、资产变更流程等，关联特定资产数据（端口、告警、运维记录、漏洞修复情况等），提供特定资产多维度视角。

3.5.2 漏洞管理子应用

也可称为隐患治理模块，主要面向漏洞子库定制流程，实现信息化隐患治理的全过程管理。

3.5.3 威胁管理子应用

统一汇集各类安全类大数据，通过威胁建模、情景关联、智能研判、协同处置、设备联动等能力，实现统一的攻击检测分析、违规行为发现、安全事件响应和态势感知预警。

3.5.4 运维管理子应用

利用接口调用或界面集成的方式纳管现存运维平台，而非完全重新设计开发。提高项目的开发效率，确保用户体验的连续性。

3.5.5 合规管理子应用

用于网络安全合规领域，以信息系统等级保护作为主要管理目标，内容涉及系统的等级保护和备案状态、等级保护信息概览、过程管理以及合规状态的展示等。

3.6 业务流程分拨模块

建设支撑安全及运维工作流转的统一流程引擎，提供业务流程编排、业务流程集成及扩展、事件分拨和消息通知等能力，形成监控告警、事件管理、变更管理、风险管理一体化的安全运维业务调度枢纽，解决业务分类的问题。

3.7 门户展示模块

一是提供安全态势和运行态势综合监控大屏视图，全面掌握安全运行状态。二是实现指挥调度功能，针对工单、问题、故障事件处置，结合实时数据分析，协助管理人员准确掌握事件风险及危害级别，动态指挥、资源综合调度，实现高效的跨层级协同作战。三是建设个人工作台，提供整体视图从运营分析、安全管理、安全运维三个维度分类展现工作。

4 发展

建成的平台，已具备对下联系统、平台数据的采集汇总功能。安全与运维大数据的集中，有了数据分析、挖掘的基础，同时与各类设备的通信集成，使平台具备了进一步拓展自动化运维与脚本编排（SOAR）的能力，可以进一步提升平台的功能。

4.1 人工智能（AIGC）

基于平台的数据底座和实网运维数据，开展智能事件研判、智能告警挖掘、智能事件处置、AI 知识助手等方向的持续训练。可利用知识图谱、语音识别等技术就智能事件研判、智能告警挖掘、智能事件处置、AI 知识助手等方向开展深化研究。

4.2 自动化运维与自动化编排 (SOAR)

自动化运维技术是自动逻辑分析、自动诊断、自动执行的运维技术。相对于传统手动运维有很多优势，可实现快速修改与部署，降低运维成本等 [2]。通过集成运维工具，可以实现快速部署和修改，减少重复作业，提升运维效率。

在安全防护方面，探索自动化编排（SOAR）响应与处置跟踪，包括自动化编排信息总览、状态分布情况、剧本执行情况统计等内容。进一步提升平台对整体信息化系统的安全管控能力。

5 结语

网络安全与运维协同运行是提升信息化运营效率的有效途径，通过建设一体化平台，整合安全与运维技术力量，不仅可实现资源和信息的有效共享，还可提升整体的运维效率和安全能力 [3]。一体化平台集中监控和管理能力，使企业能够更有效地对抗和管理网络威胁。同时，集成的框架使其能够持续发展，适应快速变化的信息技术环境，支持企业信息化长期战略。

参考文献

[1] 周晔.信息化运维与网络安全管理措施改进研究[J].保密科学技术,2023(21).

[2] 熊毅.企业网络自动化运维安全解决方案研究[J].网络安全技术与应用,2024(6).

[3] ITIL 4服务管理认证考试指南（ITIL Foundtion ITIL 4 Edition）[Z].