安全能力大集中模式下的运行保障能力成熟度评估方法研究

陈丛笑 程从凤 张春明
航天通信中心，中国·北京 100830

摘 要：在全球数字化转型加速与地缘政治冲突加剧的双重背景下，大型企业网络安全防御体系面临严峻挑战。为提升安全防御效能，大型企业普遍通过整合分散的安全资源构建集中化安全管理模式，然而该模式在提升响应效率的同时，也因管理复杂度陡增而面临运行保障能力难以量化评估的瓶颈。本研究基于 CMMC、C2M2 等国际安全能力成熟度模型，结合 ITSS 信息技术服务等标准，创新性构建三维评估框架：以运行保障能力成熟度级别为纵轴，以安全保障框架要素为横轴，通过将安全能力大集中模式下的运行保障能力拆解为多工作域，建立统一的成熟度评估模型。该模型为支撑大型企业安全运行保障能力的动态评估与持续优化，提供可量化、可落地的实施路径。

关键词：网络安全；成熟度模型；运营体系；量化评估

Research on the Maturity Evaluation Method of Operational Support Capability in the Mode of Centralized Security Capability

Chen Congxiao Cheng Congfeng Zhang Chunming
Aerospace Communication Center, Beijing, 100830, China

Abstract: Against the dual background of accelerated global digital transformation and intensified geopolitical conflicts, the network security defense system of large enterprises is facing severe challenges. To enhance the effectiveness of security defense, large enterprises generally build a centralized security management model by integrating dispersed security resources. However, while this model improves response efficiency, it also faces the bottleneck of difficulty in quantitatively evaluating operational support capabilities due to the sudden increase in management complexity.This study is based on international security capability maturity models such as CMMC and C2M2, combined with ITSS information technology service standards, and innovatively constructs a three-dimensional evaluation framework: with the maturity level of operational support capability as the vertical axis and the elements of security support framework as the horizontal axis, a unified maturity evaluation model is established by decomposing the operational support capability under the centralized mode of security capability into multiple work domains. This model provides a quantifiable and implementable implementation path to support the dynamic evaluation and continuous optimization of the security operation guarantee capability of large enterprises.

Keywords: Network security; Maturity model; Operational system; Quantitative evaluation

0 前言

网络安全成熟度评估已成为企业应对数字化威胁的核心工具，其重要性不仅体现在风险防控层面，更深刻影响着组织的战略决策与资源分配。Rea-Guamán A M[1] 的系统综述指出，2017 年前缺乏专注网络安全的成熟度模型，多数为通用框架（如 CMMI）的改编版。在识别与分析的主流网络安全成熟度评估模型中，SSE-CMM[2,3] 为高频引用模型，但其本质是信息安全框架而非专门的网络安全模型，不完全适用网络安全领域；COBIT 框架 [4] 强在 IT 治理，但弱在威胁狩猎等网安专项能力；C2M2[5,6] 为面向能源、关键基础设施的成熟度评估模型；Rea-Guamán A M 提出以上 78% 的模型未考虑组织规模差异，在安全能力集中模式下的网络安全成熟度评估模型存在缺口。

随着大型企业推行安全能力大集中模式（整合资源、统一策略、集中数据分析），面临保障机制复杂化、跨域协同难度高等挑战。因此，建立与之匹配的运行保障能力成熟度评估模型，也是保障集中化安全效能持续优化的重要需求。

1 安全运行保障能力成熟度评估模型

本研究基于类 CMM 等安全能力成熟度模型，结合 ITSS 信息技术服务标准，创新性构建三维评估框架，如图 1 所示，以运行保障能力成熟度级别为纵轴，覆盖初始执行级、基础运维级、管理体系级、评估量化级和持续优化级五个成熟度等级；以安全保障框架要素为横轴，解构组织架构、流程规范、技术能力、平台工具四大核心维度；以各类工作领域为剖面，划分资产管理、安全威胁监测、威胁情报管理、应急响应、重保演练等多个核心防护场景。通过将安全能力

大集中模式下的运行保障能力拆解为多工作域，并进一步细化为标准化基本实践，建立统一的成熟度评估模型。

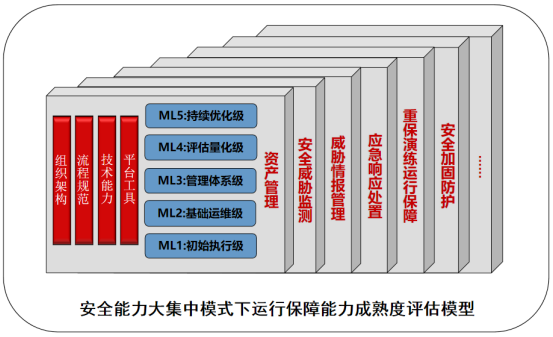

图 1 运行保障能力成熟度评估模型

2 成熟度级别定义

如图 2 所示，本模型包含的五个成熟度级别，各成熟度级别定义如下。

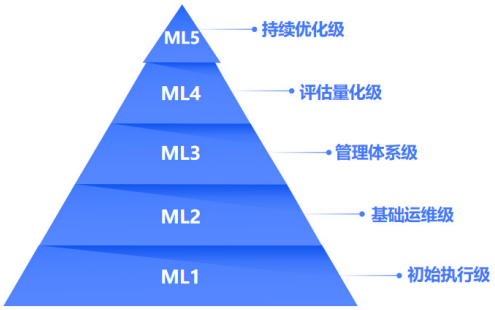

图 2 成熟度级别定义

2.1 初始执行级

安全能力分散在各子 / 分公司或部门，依赖本地化、临时性措施，安全响应被动，无统一流程或标准，依赖个人经验。

2.2 基础运维级

制定了基本的安全计划，但执行依赖本地团队，缺乏强制约束力，子 / 分公司仅有基础运维管理制度，安全能力参差不齐。

2.3 体系管理级

建立全域统一的安全管理体系（制度、流程、技术栈），设立能力集中的安全运营中心，安全资源统筹规划，安全团队集中调度，实现流程制度化。

2.4 评估量化级

基于数据建模量化安全效能，动态调整资源分配，优化集中化策略，建立较大规模安全团队，定义统一安全度量指标体系，量化安全风险，实现预测性分析

2.5 持续优化级

集中化安全能力实现弹性扩展，形成自适应演进机制，安全能力长期保持行业一流，能够对安全业务发展方向准确识别和实现自身需求。

3 安全保障框架要素

人员（people）、过程（process）、技术（technology）和资源（resource）为 IT 服务的四大核心组成，本方法基于 ITSS 标准，构筑作为大型企业集中化安全中心的运行保障核心四要素，形成从组织架构、流程规范、技术能力、平台工具四个能力类型出发量化过程能力的评估模型。

①组织架构：组织体制对于设计并实现安全运营体系的保障能力，如架构调整、资源保障、职责分配、业绩考核等。

②流程规范：安全运营过程相关的流程的规范性、完善性和有效性。

③技术能力：安全运营过程相关人员的专业能力和安全通识能力，以及相关的能力建设。

④平台工具：支撑安全运营中人员与流程运转以实现安全功能的平台或工具。

4 工作域实践内容

基于大型集团网络安全运营中心的实践，梳理出若干核心安全运营工作域。每个工作域聚焦一类独立且专业的工作范畴，各域逻辑清晰、相互独立，但共同保障整体安全运行效能。常见安全集中化管理的企业中的工作域主要包括：资产管理、安全威胁监测、威胁情报管理、重保演练、安全加固、应急响应、安全集成、风险评估等。以下为最常见、最主要的四个工作域在各成熟度级别下的主要实践内容。

4.1 资产管理成熟度

4.1.1 初始执行级

组织体制：安全策略包含资产管理。

流程规范：建立并维护资产清单。

技术能力：人员了解基本的资产清单维护过程。

平台工具：无明确要求。

4.1.2 基础运维级

组织体制：各子 / 分公司配合进行资产管理。

流程规范：明确资产责任人，建立资产上下线管理流程，建立资产基线并有计划地发现异常资产。

技术能力：能够识别异常资产出现的原因。

平台工具：无明确要求。

4.1.3 体系管理级

组织体制：设计覆盖资产管理的安全体系，资产管理纳入集团考评体系，专职团队承担资产管理。

流程规范：基于业务情况建立资产分类分级管理规范和流程，建立资产全生命周期管理流程，资产管理流程标准化并覆盖全部相关方，资产基线覆盖组件、版本、配置等详细信息并实施管理。

技术能力：能够识别异常资产情况出现的原因。

平台工具：资产基线信息模板，基于资产基线发现异常资产的技术。

4.1.4 评估量化级

组织体制：资产管理过程的改进效果纳入考评体系，明确业务发展目标。

流程规范：针对各项提升资产管理能力的过程建立度量指标，将业务发展目标拆解为量化的资产管理优化目标，评估知识库对资产管理的提升作用。

技术能力：人员具备针对运营过程建立度量模型的能力。

平台工具：准确、全面记录资产管理执行和改进过程数据的系统，提供数据分析能力的系统。

4.1.5 持续优化级

组织体制：设立运营优化岗位，具有长期安全目标。

流程规范：基于业务和数据分析改进资产管理运营机制，持续评估资产管理提升机制的有效性，持续分析业务演化对资产管理的需求。

技术能力：运营体系优化设计能力。

平台工具：资产运营体系优化支撑平台。

4.2 安全威胁监测成熟度

4.2.1 初始执行级

组织体制：安全策略包含基本的安全威胁监测要求。

流程规范：建立并维护监测事件及处置清单。

技术能力：了解基本的安全威胁概念，能够识别常见的安全事件和异常行为。

平台工具：无明确要求。

4.2.2 基础运维级

组织体制：明确安全威胁监测的职责分工，各单位配合监测响应工作。

流程规范：建立标准化的安全威胁监测流程，规范监测步骤和方法、制定安全事件的报告和处理流程。

技术能力：人员具备处理常见安全事件的能力，能按照流程进行处置响应。

平台工具：基本的监管平台以及日志查看和分析工具。

4.2.3 体系管理级

组织体制：建立专职的安全威胁监测团队，明确团队职责和目标；建立安全事件的分级分类和升级机制，确保重大事件及时处理。

流程规范：建立统一的安全监测标准和指标，规范监测数据收集和分析方法。

技术能力：人员具备深入的安全威胁分析技能，能够识别复杂和高级的安全威胁，定期培训，不断提升人员专业能力。

平台工具：部署先进的安全监测系统（如入侵监测系统等），与其他安全系统（如上网行为管理、终端安全管理、日志审计系统、防火墙）等集成，实现协同防御。

4.2.4 评估量化级

组织体制：将安全威胁监测与业务目标和风险管理紧密结合，定期向集团汇报与展示，支撑决策；制定全面的安全威胁监测策略和计划，覆盖网络、主机、应用等层面，与各网络中心、各单位深度合作，分享和获取最新的安全威胁信息和最佳实践。

流程规范：建立安全威胁监测的数据分析和报告机制，提供可视化的安全态势；制定量的安全监测绩效指标（KPI），如检测率、响应时间、误报率等，对应于各单位制定威胁闭环率、威胁闭环时间等。

技术能力：人员具备深入的安全威胁分析技能，能够识别复杂和高级的安全威胁，熟练使用专业的安全监测工具和平台，进行安全事件分析和溯源。

平台工具：部署更为先进的安全监测系统，配合大数据、人工智能等自动化、智慧化能力。

4.2.5 持续优化级

组织体制：建立持续优化的安全威胁监测机制，及时应对新型威胁和攻击手段，安全威胁监测深度融入组织的业务流程和文化中，形成安全自驱力。

流程规范：定期评估和优化监测流程和策略，基于数据驱动改进，实现安全威胁监测的自动化和智能化，具备自适应和自学习能力。

技术能力：人员具备创新意识和能力，能够研究和应用前沿的安全技术和方法，培养全面的业务理解力，能够在业务创新中嵌入安全监测要求。

4.3 威胁情报管理成熟度

4.3.1 初始执行级

组织体制：在安全策略中简单提及威胁情报的获取和处理方式。

流程规范：被动获取公开的威胁情报，主要依赖公开渠道，未经筛选地接收威胁情报信息。

技术能力：对威胁情报的概念和重要性有基本了解。

平台工具：无明确要求。

4.3.2 基础运维级

组织体制：指定人员或团队负责威胁情报的收集和分发，重点关注与自身业务相关的威胁情报。

流程规范：制定威胁情报接收和处理流程，明确威胁情报的收集、分析、传递、响应等基本流程。

技术能力：能够解读威胁情报的基本内容，识别一般性的安全威胁。

平台工具：利用公开的情报源和简单的工具收集情报。

4.3.3 体系管理级

组织体制：组建专业团队，负责全面的威胁情报管理工作，将威胁情报管理作为安全战略的重要组成部分。

流程规范：根据情报的类型、重要性、紧急程度进行分类管理，从情报的获取、验证、分析、应用到反馈，形成闭环管理。

技术能力：安全人员接受专业培训，具备深度分析复杂情报的能力，能够评估情报对组织的潜在威胁，制定相应的安全防护策略，行业内共享情报分析经验和知识。

平台工具：部署先进的安全监测系统，与情报管理系统或平台集成，实现协同防御。

4.3.4 评估量化级

组织体制：设定量化的威胁情报管理目标，确保威胁情报管理与业务目标同步，支持业务的安全运营。

流程规范：量化评估情报利用效果，建立指标，评估情报在威胁检测、响应中的实际效果，持续优化情报管理流程。

技术能力：人员具备数据分析和挖掘能力，能够从大量威胁情报中提取汇总出有价值的情报。能够根据情报分析结果，及时调整安全策略和防护措施。

平台工具：将情报与防火墙、IDS/IPS 等安全设备联动，实现自动化防护以及威胁情报管理、分析类工具。

4.3.5 持续优化级

组织体制：制定长期规划，不断优化威胁情报管理体系。

流程规范：基于情报预测未来威胁趋势，提前部署防御措施；引入最新技术和方法，不断革新情报管理模式

技术能力：人员具备创新思维，能够开拓新的情报分析方法和应用场景；引领情报分析的发展方向

平台工具：利用 AI 和机器学习技术，提升情报分析的智能化水平；开发适合自身需求的情报分析和管理工具，实现高度定制化。

4.4 应急响应处置成熟度

4.4.1 初始执行级

组织体制：仅有基本的人员管理制度。

流程规范：仅被动响应安全事件。

技术能力：人员了解应急响应的目的和重要性。

平台工具：无明确要求。

4.4.2 基础运维级

组织体制：安全策略包含应急响应的规则制度，应急响应流程、建立安全事件通报和处罚机制。

流程规范：建立安全事件处置清单、建立安全事件的响应和恢复流程，明确响应时间和步骤、明确各单位安全事件的责任人。

技术能力：能够识别和响应常见的安全事件，具备基本的事件调查和取证能力。

平台工具：基本的工单系统，用于记录、分配和跟踪安全事件的处理进展。

4.4.3 体系管理级

组织体制：设计覆盖应急响应的安全体系，并将其纳入组织的管理制度，具有专职的应急响应团队，明确团队结构、职责和工作流程。

流程规范：基于业务情况，建立安全事件分级标准，明确不同级别事件的影响范围和处理优先级，标准化应急响应流程，建立全面的应急响应预案，涵盖事件检测、报告、分析、遏制、消除、恢复和事后评估，建立安全事件全生命周期管理流程。

技术能力：能够评估安全事件对业务的影响，制定业务连续性和灾难恢复计划，能够发现应急响应制度存在的问题，提出改进建议。

平台工具：建立覆盖应急响应的知识库，收集各类安全事件的处理经验和最佳实践。

4.4.4 评估量化级

组织体制：将平均修复时间、事件复发率纳入 KPI 考核；设立独立应急管理中心，推动跨组织协同响应。

流程规范：量化应急处置指标（如首次响应时间≤ 5 分钟、处置成功率≥ 95% 等）。

技术能力：人员掌握攻击链分析，预测高危场景，威胁情报融合分析，驱动精准响应。

平台工具：通过 SOAR 等平台实现剧本化响应，可视化展示应急效能仪表盘。

4.4.5 持续优化级

组织体制：团队结构高度协同、灵活，具备高度专业化的技能分工；建立与外部安全组织、监管机构、执法机构的顺畅协作渠道；定期进行组织结构评估优化。

流程规范：流程高度精细化、情境化（基于不同事件类型、不同影响等级）。定期迭代防御策略，定期更新攻击链推演剧本；流程融入业务连续性 / 灾难恢复考虑。

技术能力：具备对高级持续性威胁（APT）的复杂分析能力，能进行有效的大规模事件响应。

平台工具：构建自适应响应平台，集成 SOAR+AI 功能，实现从告警到处置的全流程自动化。

5 结论

本研究针对安全能力大集中模式下因管理复杂度激增导致的运行保障能力难以量化问题提出三维评估框架。通过纵向成熟度分级（初始执行→持续优化）、横向能力解构（组织架构 / 流程规范 / 技术能力 / 平台工具）、剖面工作域细分（资产管理 / 威胁监测 / 应急响应等），实现对安全能力集中模式下复杂运行保障能力的结构化拆解。将抽象的安全能力转化为可观测、可度量的标准化实践，支持企业进行差距定位，转向持续能力演进。

参考文献：

[1] Rea-Guamán A M, Sanchez-Garcia I D, San Feliu T, et al. Maturity models in cybersecurity: A systematic review[C]//12th Iberian conference on information systems and technologies (CISTI). IEEE,2017.

[2] ISO/IEC 21827:2008 Information technology — Security techniques — SSE-CMM[Z].

[3] A I Hohan, M Olaru, I C Pirnea. Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles[J]. Procedia Economics and Finance,2015,32(15):352-359.

[4] Y Goksen, E Cevik, H Avunduk. A Case Analysis on the Focus on the Maturity Models and Information Technologies[J]. Procedia Economics and Finance,2015,19(15):208-216.

[5] R M Adler. A dynamic capability maturity model for improving cyber security[J]. IEEE International Conference on Technologies for Homeland Security (HST),2013:230-235.

[6] J Payette, E Anegbe E. Caceres and S. Muegge, Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects,2015:26-34.