



中华人民共和国国家标准

GB/T 45940—2025

网络安全技术 网络安全运维实施指南

Cybersecurity technology—
Implementation guide of cybersecurity operation and maintenance

2025-08-01 发布

2026-02-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 概述 2

 5.1 网络安全运维目标 2

 5.2 网络安全运维参考框架 2

6 网络安全运维条件 3

 6.1 网络安全运维提供方 3

 6.2 网络安全运维人员 3

 6.3 网络安全运营中心 4

7 网络安全运维业务建立 4

 7.1 网络安全运维模式 4

 7.2 网络安全运维实施内容 5

 7.3 网络安全运维业务建立过程 6

8 网络安全运维实施 6

 8.1 运维实施过程 6

 8.2 运维管理 7

 8.3 识别 8

 8.4 防护 10

 8.5 监测分析 11

 8.6 事件处置 14

 8.7 协同 15

 8.8 运维效果评估 16

附录 A（资料性） 网络安全运维能力评估 19

 A.1 评估模型 19

 A.2 评估内容 20

 A.3 评级方法 21

附录 B（资料性） 网络安全运营中心建设 22

 B.1 建设模型 22

 B.2 场所条件 28

 B.3 平台与工具 29

参考文献 31

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国信息安全测评中心、杭州安恒信息技术股份有限公司、国家信息中心、北京神州绿盟科技有限公司、北京长亭科技有限公司、奇安信科技集团股份有限公司、北京梆梆安全科技有限公司、中国信息通信研究院、北京天融信网络安全技术有限公司、三六零数字安全科技集团有限公司、新长城科技有限公司、清华大学、中国联合网络通信集团有限公司、中国科学院信息工程研究所、杭州迪普科技股份有限公司、国网思极网安科技(北京)有限公司、华能信息技术有限公司、深信服科技股份有限公司、北京赛西科技发展有限公司、上海三零卫士信息安全有限公司、中福彩科技发展(北京)有限公司、深圳市博通智能技术有限公司、罗克佳华科技集团股份有限公司、安天科技集团股份有限公司、广州中软信息技术有限公司、北京知其安科技有限公司、杭州网易智企科技有限公司、北京威努特技术有限公司、北京升鑫网络科技有限公司、北京灰度科技有限公司、天翼云科技有限公司、广东网安科技有限公司、宁波和利时信息安全研究院有限公司、黑龙江安信与诚科技开发有限公司。

本文件主要起草人：王琰、杨婧婧、袁明坤、陈星、田丽丹、刘蓓、杨莹、曹嘉、李昀磊、许玉娜、田宝松、杨坤、张龙、马玉、陈祥喜、赵相楠、方宁、代杭旅、杨家海、白峻、王馨茹、王雨薇、云瀚、刘吉林、潘中英、崔磊、刘彪、卫世光、聂君、王喜伟、申东胜、周凯、周灵军、谢美程、周森、程度、卢志刚、李玮、辛晨、魏书山、曹静、崔馨、杨亮。

网络安全技术

网络安全运维实施指南

1 范围

本文件提出了网络安全运维参考框架、网络安全运维提供方和运维人员条件和运维业务建立过程,给出了运维管理、识别、防护、监测分析、事件处置、协同和效果评估等网络安全运维主要工作环节实施内容。

本文件适用于网络安全运维提供方和需求方。用于网络安全运维的实施提供指导,并为网络安全运维需求方、第三方机构对网络安全运维实施效果和网络安全运维能力进行评估提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

- GB/T 20984 信息安全技术 信息安全风险评估方法
- GB/T 20985.2 信息技术 安全技术 信息安全事件管理 第2部分:事件响应规划和准备指南
- GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南
- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 24363 信息安全技术 信息安全应急响应计划规范
- GB/T 25069—2022 信息安全技术 术语
- GB/T 28827.3 信息技术服务 运行维护 第3部分:应急响应规范
- GB/T 32914—2023 信息安全技术 网络安全服务能力要求
- GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
- GB/T 39786 信息安全技术 信息系统密码应用基本要求
- GB/T 42446 信息安全技术 网络安全从业人员能力基本要求
- GB/T 43698—2024 网络安全技术 软件供应链安全要求
- GB/T 45577 数据安全技术 数据安全风险评估方法

3 术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

网络安全运维 cybersecurity operation and maintenance

组织为抵御网络空间安全威胁,控制网络安全风险,确保业务持续、稳定运行,保证业务以及承载数据的保密性、完整性和可用性,统筹技术、流程、人员等要素,持续开展管理、识别、防护、监测分析、事件处置、协同等工作的一种网络安全服务方式。

4 缩略语

下列缩略语适用于本文件：

APT:高级持续性威胁(advanced persistent threat)

CNAME:别名记录(canonical name)

DDOS:分布式拒绝服务攻击(distributed denial of service attack)

DNS:域名系统(domain name system)

IP:互联网通信协议(Internet Protocol)

MSS:托管安全服务(managed security service)

SaaS:软件即服务(software as a service)

SLA:服务级别协议(service level agreement)

SOC:安全运营中心(security operations center)

5 概述

5.1 网络安全运维目标

网络安全运维的目标是为组织提供高效、全面的安全保障,确保组织的业务稳定可靠运行,信息系统能够抵御各种形式的网络攻击,提高用户和员工的安全意识,以实现更高水平的网络安全防护,具体包括:

- a) 保障业务持续发展:确保系统的连续性和稳定性,在面临挑战和威胁时保障业务的正常运行;
- b) 使安全能力达到组织、机构和设施的需求:不同的组织、机构和设施对安全能力的要求有所不同,安全运维提供方根据这些需求来制定和实施相应的安全策略和措施,确保其安全能力能够满足要求;
- c) 使组织、机构和设施的信息安全风险处于可接受的范围:网络安全运维提供方帮助组织、机构和设施识别、评估和管理所面临的信息安全风险,并采取必要的措施来降低风险;
- d) 确保网络安全能力持续有效:通过网络安全运维,防范各种网络安全威胁,确保网络的安全性和可用性,使网络系统的安全性得到持续维护和提升;
- e) 满足安全监管要求:网络安全运维提供方帮助组织、机构和设施满足各种安全监管要求,并提供必要的证明材料,如审计报告、安全漏洞修补证明等,确保其信息安全管理符合相关法规和标准。

5.2 网络安全运维参考框架

网络安全运维参考框架包含了网络安全运维条件、网络安全运维业务建立、网络安全运维实施三个方面的内容:

- a) 网络安全运维条件包括了开展网络安全运维活动运维提供方、运维人员、运营中心具备的基本条件;
- b) 网络安全运维业务建立包括了开展网络安全运维的三种模式,以及在确定运维模式后,安全运维业务的建立过程;
- c) 网络安全运维的实施包括运维管理、识别、防护、监测分析、事件处置、协同和效果评估七个环节。

网络安全运维参考框架如图 1 所示。

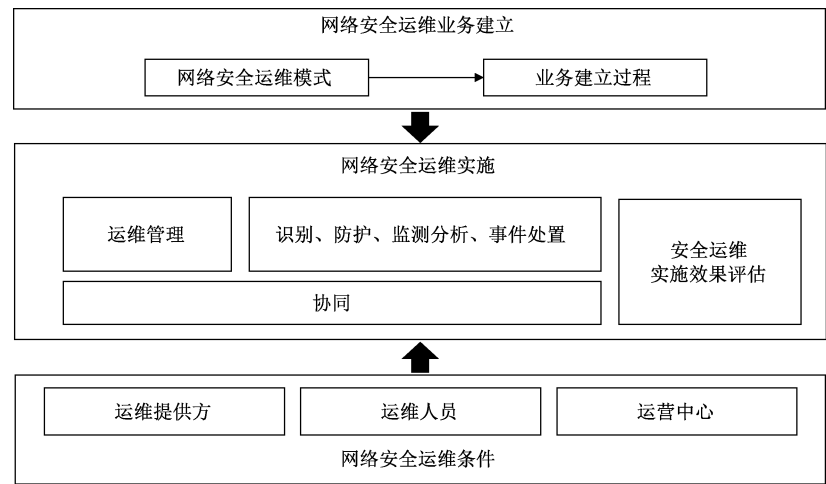


图 1 网络安全运维参考框架

6 网络安全运维条件

6.1 网络安全运维提供方

网络安全运维提供方向网络安全运维需求方提供网络安全运维时,满足 GB/T 32914—2023 中第 5 章对网络安全服务机构的一般要求。如向对网络安全运维有更高要求的服务需求方(如党政机关、关键信息基础设施运营者等)提供网络安全运维时,还需满足 GB/T 32914—2023 中第 6 章对网络安全服务机构的增强要求。网络安全运维能力评估的模型、内容和方法见附录 A。

6.2 网络安全运维人员

6.2.1 需求方参与网络安全运维的人员

需求方参与网络安全运维的人员具备的条件包括:

- a) 理解与本单位网络安全目标相关的法律法规、政策和标准;
- b) 了解本单位网络安全运维的目标和方法,网络安全运维组织架构,网络安全运维角色和职责;
- c) 掌握既有网络情况,能够明确软硬件及网络扩容需求,能够定义和评估业务系统面临的安全风险;
- d) 根据应用系统特点和运行需求,充分与安全运维提供方人员沟通和协作,制定网络安全运维实施方案;
- e) 能够识别与信息系统相关的资产,构建以资产为核心的网络安全风险管理机制。

6.2.2 网络安全运维提供方人员

网络安全运维提供方人员是指向运维需求方提供安全运维服务的人员,宜符合下列条件。

- a) 根据不同的工作角色,安全运维提供方人员除满足 GB/T 42446 中关于网络安全运营类人员的要求外,还宜具备下列技术和能力,包括但不限于:
 - 1) 能够识别与安全运维工作范围相关的所有信息系统资产;
 - 2) 能够识别网络和系统的访问控制存在的风险,并能提供对应的整改建议;

- 3) 基于信息安全策略,制定备份策略,保证备份的有效性和可靠性;
 - 4) 通过全面收集并管理信息系统及相关设备的运行日志,帮助排查定位和溯源网络安全攻击;
 - 5) 定期借助漏洞扫描工具对信息系统及其软硬件系统存在的漏洞进行扫描,发现存在的脆弱性,并提供处置建议;
 - 6) 建立监视、发现、分析和报告信息安全事态和事件流程,流程中明确对不同级别事件的响应时间要求,确保快速、有效和有序地响应信息安全事件。
- b) 签订保密协议,向有更高要求的需求方(如党政机关、关键信息基础设施运营者)提供服务时对其进行安全背景审查,确保参与网络安全运维的人员安全可靠。

6.3 网络安全运营中心

网络安全运营中心是为抵御网络安全威胁,保障组织网络基础设施稳定运行,有机结合人员、流程和技术,提供网络安全运维的组织单元。网络安全运维的组织架构一般包括安全运维领导小组、运维管理组、运维工作组、下属单位运维组等,所有组织单元中包含相应的岗位和人员。安全运维领导小组总负责人通常由组织的首席安全官或首席信息安全官担任,运维工作组可包含一个或多个工作组。已经具备自主网络安全威胁管理和漏洞管理能力的组织和机构,根据组织的实际需求和基础能力,宜考虑建立网络安全运营中心。网络安全运营中心的建设在满足国家相关法律法规,以及行业监管要求的前提下,宜考虑以下方面:

- a) 广泛参与:组织和机构的相关信息技术和业务部门宜广泛参与;
- b) 最小业务影响:组织和机构的网络安全运营中心建设和实施在达成组织安全目标的前提下,将对业务可能造成的影响降低到最小;
- c) 持续改进:组织和机构不断提升网络安全运营中心的安全能力和运维水平;
- d) 自身安全:组织和机构网络安全运营中心的建设保障自身安全性和业务连续性,建立相适应的网络安全管理、数据安全管理机制,并将供应链安全、外包安全等因素纳入到自身安全建设的考虑范围之中。

基于三种不同模式开展网络安全运营中心建设的内容见附录 B。

7 网络安全运维业务建立

7.1 网络安全运维模式

网络安全运维模式主要包括以下三种类型。

- a) 全自建网络安全运维模式:网络安全运维需求方具备完善的安全运维人员配置、管理机制和人才培养机制,整合安全防护技术、安全运维工具与平台和人员等要素,建立网络安全监测、分析、处置、应急等网络安全运维流程,自主建设 SOC;一般来说,对安全性和数据保护的要求较高,具备足够的安全资源投入,能够持续有效网络安全运维的网络安全运维需求方,选择自主建设 SOC。
- b) 联合网络安全运维模式:网络安全运维需求方联合网络安全运维提供方共同建设 SOC,整合安全运维技术、平台、工具、人员等要素,建立网络安全监测、分析、处置、应急等网络安全运维流程,网络安全运维提供方为网络安全运维需求方提供驻场网络安全运维。
- c) 全托管网络安全运维模式:基于托管安全服务(MSS)开展全托管网络安全运维,依靠网络安全运维提供方建设的 SOC,通过云平台或远程管理系统,管理组织 IT 资产的安全信息、管理安

全工具、监测和改善组织的安全状况，识别、检测、分析和响应组织所面临的网络安全事件，以满足对安全人员、技术和流程外包的需要。

7.2 网络安全运维实施内容

基于组织对网络安全运维的具体要求和网络安全运维参考框架，网络安全运维实施的基本工作内容如表 1 所示。网络安全运维提供方结合网络安全运维实践，选择确定网络安全运维实施内容，并持续更新。

表 1 网络安全运维实施基本工作内容

序号	工作内容
A	运维管理
A-1	制度管理
A-2	流程管理
A-3	资产管理
A-4	工具管理
A-5	报告管理
A-6	审计管理
A-7	境外运维管理
B	识别
B-1	业务识别
B-2	资产识别
B-3	风险识别
B-4	威胁信息收集
B-5	合规自评估
C	防护
C-1	设备安全运维
C-2	安全加固
C-3	数据安全防护
C-4	密码应用安全
D	监测分析
D-1	网络流量监测
D-2	网络资产暴露面监测
D-3	终端监测
D-4	数据监测
D-5	域名安全监测



表 1 网络安全运维实施基本工作内容（续）

序号	工作内容
D-6	实时分析
D-7	深度分析
E	响应
E-1	应急预案
E-2	应急响应
E-3	处置与恢复
E-4	事件总结
F	协同
F-1	人员能力提升
F-2	供应链安全
F-3	信息协同共享
G	效果评估

7.3 网络安全运维业务建立过程

在实施网络安全运维之前,网络安全运维供需双方协商创建网络安全运维表单,表单示例如表 2 所示,创建过程包括:

- a) 根据需求方的实际情况,协商确定网络安全运维模式;
- b) 网络安全运维提供方根据表 1 的内容,选择安全运维内容并添加组织特需的安全运维内容来确定网络安全运维目录;
- c) 根据 SLA 确定运维目标,为运维目录中的每项运维内容建立一个配置文件,包括:所有者、运维团队角色、职责以及运维模式。

表 2 网络安全运维表单示例

服务项目名称	运维模式	运维目录与目标	项目配置文件
运维服务项目 1	自主型	运维目录和 SLA1	配置文件 1
运维服务项目 2	托管型	运维目录和 SLA2	配置文件 2
运维服务项目 3	托管型	运维目录和 SLA3	配置文件 3
运维服务项目 4	联合型	运维目录和 SLA4	配置文件 4

8 网络安全运维实施

8.1 运维实施过程

网络安全运维的实施过程如图 2 所示。运维管理对网络安全运维的整体活动进行规划和管理,考

考虑组织网络安全长期改进需要做出的决策和进行的投入,提出网络安全运维整体方案;协同指通过网络安全运维活动相关方组织内外部的协调与协作,通过威胁信息共享、供应链安全管理等活动以提高网络安全运维的效能与安全防护水平,运维管理和协同是针对网络安全风险防范的常态化长期活动,在网络安全运维活动中属于持续性过程。识别、防护和监测分析和事件处置四个环节是针对网络安全事件进行响应和处置的应急性活动,在网络安全运维活动中是一个快速响应过程。效果评估是在网络安全运维过程中,基于 SLA 对运维实际效果进行评估,根据效果评估情况进一步改进网络安全运维的管理和实施水平。

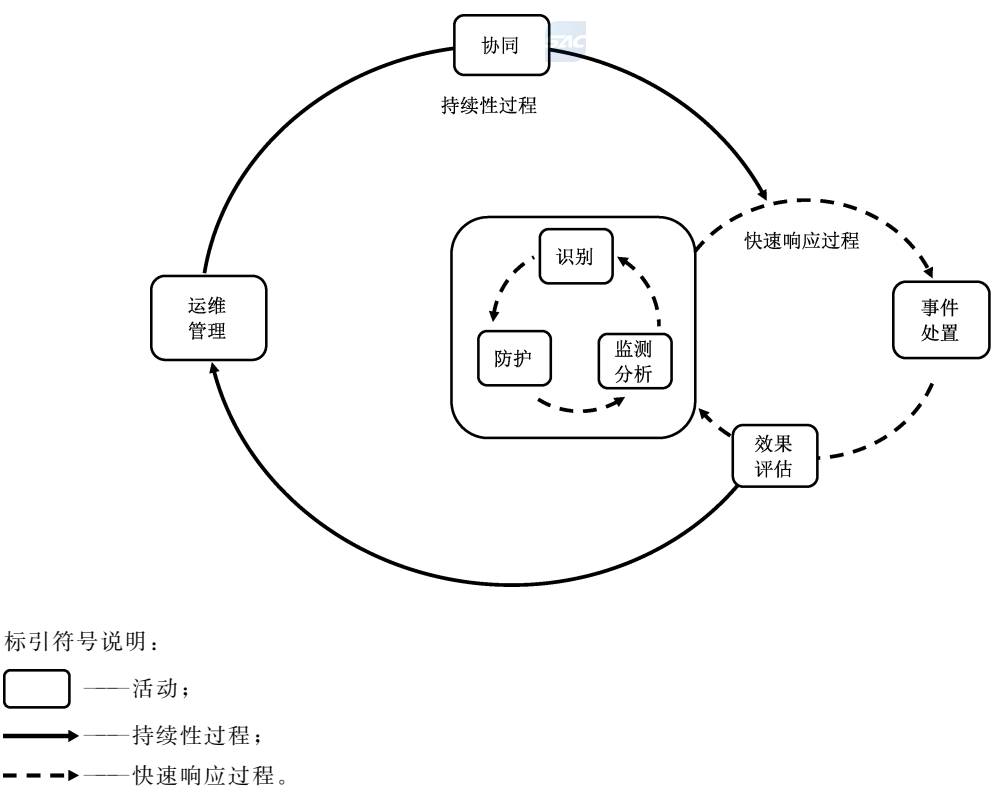


图 2 网络安全运维实施过程

8.2 运维管理

运维管理是对与运维活动有关的制度、流程、资产、工具、报告等进行管理的过程。目的是确保网络安全运维活动可持续性和稳定性。具体包括以下内容：

- a) 制度管理:按照 GB/T 22239 相关要求,建立网络安全运维工作领导小组,编制保密管理、介质管理、设备安全、监测预警、网络安全、系统安全、安全培训、备份与恢复、变更管理等相关制度,并制定网络和信息安全突发事件应急预案,规范运维团队日常行为,降低网络安全风险;
- b) 流程管理:建立安全运维作业流程,指导和规范运维团队开展安全运维工作,包括安全监测流程、风险处置流程、应急响应流程、策略变更流程、安全加固流程、信息共享流程、威胁信息运维流程等;
- c) 资产管理:编制并保存运维需求方的资产清单,资产属性包括资产名称、资产编号、IP 地址、序列号、所处位置、责任部门、责任人、重要程度等;并根据资产的重要程度进行资产和线路标识管理;资产管理对象包括重要网络设备、安全设备、主机系统、业务系统、门户网站、邮箱及接口服务等;

- d) 工具管理:编制运维工具清单,包括工具名称、类型、型号、版本号、作用、存放位置、维护部门等信息,定期更新维护,提升安全运维效率;
- e) 报告管理:运维报告包括不限于各类日报、周报、月报、年报、建议书、安全事件报告、总结分析报告等,建立报告审核流程,确保报告格式和内容的规范性、有效性;
- f) 审计管理:对运维需求方的运维操作进行审计、查阅和回放,确保所有操作行为可审计、可追溯;
- g) 境外运维管理:如确需境外运维(包括境外提供方在境内开展运维及境内提供方在境外开展运维),符合当地法律法规要求及相关规定。

8.3 识别

8.3.1 概述

通过业务识别、资产识别、风险识别、威胁信息收集和合规自评等工作,实现网络安全运维的风险趋势分析、预警和发现。

8.3.2 业务识别



业务是实现组织发展规划的具体活动,业务识别是开展网络安全运维的基础工作,包括业务的属性、定位、完整性和关联性识别。宜按照 GB/T 20984 进行业务识别,业务识别内容包括如下。

- a) 建立组织与安全运维相关的业务台账,明确业务属性,包括业务功能、业务对象、业务流程、业务范围、覆盖地域等。
- b) 识别业务在组织发展规划中的定位,包括发展规划中的职能定位、与发展规划目标的契合度、业务布局中的位置和作用、竞争关系中竞争力强弱等。
- c) 识别组织中的独立业务和非独立业务,识别组织业务与其他业务的关联关系和关联程度。如:并列关系、承接关系、直接或间接关联关系等。关联程度包括紧密关联和非紧密关联。
- d) 确认重要业务链和关键业务链,明确支撑重要和关键业务的资源分布和运行情况,从安全防护的视角,评估已识别的业务需要匹配的防护等级。
- e) 当业务范围或业务的重要性发生变化时,重新进行业务识别。

8.3.3 资产识别

资产是对组织具有价值的信息或资源,是安全策略保护的对象,也是开展体系化、精细化网络安全运维的基础。组织对资产进行全生命周期管理,建立健全资产管理制度,对资产全流程进行跟踪和管理。资产识别内容包括如下。

- a) 建立健全完善的资产管理制度,对资产上线、变更、下线等流程进行跟踪和管理,明确资产管理责任人及资产供应链。
- b) 建立健全资产台账,定期通过技术手段识别未知或新增的资产,动态确认并完善更新资产基本属性、安全属性、管理属性、指纹信息,识别资产间的关联性,绘制资产关联图谱。按照 GB/T 20984和 GB/T 22239 的要求,结合风险评估和信息系统安全等级保护备案情况,对信息资产进行分类分级和资产赋值,并在资产投入使用前完成资产纳管。采用主动或被动资产探测技术识别资产,并动态更新。
- c) 基于资产类别、资产重要性和支撑业务的重要性,确定资产防护的优先级;梳理和验证安全防护措施对资产的防护状态,同步更新资产安全防护属性信息。
- d) 定期通过技术手段感知资产属性变更,根据预设规则识别变更风险,开展安全告警、通报、处

置;对变更的敏感项进行记录和审核,以便事后审计和追溯。

- e) 根据域名、IP、端口、中间件、应用、技术架构、变更状态、业务类型(自定义)等条件对资产进行查询、统计,并能对资产进行周期变化监控。基于最小化原则,尽可能收敛互联网资产暴露面。资产转移或处置时,及时完成资产清单的更新,资产管理责任人识别可能出现的风险并予以控制,并保留相关记录。

8.3.4 风险识别

8.3.4.1 威胁识别

威胁识别主要涉及对系统或网络造成安全风险的各种因素进行识别和评估。这通常包括威胁的来源、途径和意图等,以及威胁利用脆弱性的可能性。威胁识别内容包括如下。

- a) 威胁识别内容:包括威胁来源、主体、动机、时机和频率等。
- b) 威胁来源:按照 GB/T 20984 的要求对威胁来源进行识别,同时对来自内部的威胁,包括员工恶意行为、误操作等进行识别和评估。
- c) 威胁主体:威胁主体主要包括实体和环境。实体主要包括国家、组织团体和个人,环境主要包括一般的、较为严重的和严重的自然灾害等。
- d) 威胁动机:可分为恶意和非恶意。
- e) 威胁频率:根据经验和有关的统计数据判断,综合以往安全事件报告中的威胁和频率统计、实际环境通过检测工具及日志发现的威胁和其频率统计、实际环境监测发现的威胁及其频率统计、近期公开发布的社会或特定行业威胁及其频率统计。

8.3.4.2 脆弱性识别

脆弱性是组织、系统和信息资产自身存在的。由于信息资产的脆弱性的存在具有隐蔽性,需针对需要保护的资产,识别可能被威胁利用的脆弱点,采取适当的技术或管理措施进行防范。脆弱性识别内容包括如下。

- a) 脆弱性识别:采取问卷调查、工具检测、人工核查、文档查阅、渗透测试等手段探测和识别资产在物理环境、网络结构、系统软件、应用中间件、应用系统、技术管理、组织管理等方面存在技术或管理脆弱性;根据资产价值、类型、暴露面等维度,采取不同的脆弱性探测策略。
- b) 脆弱性评估:对检测发现的脆弱性进行研判和甄别,并基于资产价值、资产暴露面类型、脆弱性严重程度、脆弱性利用难度等维度评估可能造成安全威胁的风险级别,评定脆弱性问题修复先后次序和脆弱性利用防范方式。
- c) 脆弱性管理:借助信息系统将所有安全脆弱性问题列入统一工单管理,开展通报、接收、修复、复测等工作,定期跟踪、督促修复工作进展,复测通过后关闭工单;定期或不定期组织开展安全脆弱性问题分析总结工作,调整安全策略、优化运维流程、健全完善安全管理制度。

8.3.5 威胁信息收集

汇集内、外部各种网络安全威胁相关的信息,经甄别、分类、研判、整理,辅助开展安全加固、应急处置和安全决策等安全运维工作。信息收集内容包括:

- a) 信息获取:审查并选择必要且适当的内外部各种途径来源的威胁相关信息,包括资产信息(包括但不限于与组织可能遭受的网络安全威胁相关的网络、系统软硬件、数据等)、漏洞信息、攻击信息、事件信息等;
- b) 分类研判:对获取的相关信息核验和甄别、加工完善并进行分类;

- c) 信息使用:对威胁信息进行查询查阅、数据提取分析辅助安全决策、应急响应,或基于自动化技术对威胁信息进行碰撞和关联分析开展自动化威胁处置工作,或识别、审查、清洗、处理、保护可共享的威胁信息用于信息共享。

注:信息收集过程所涉及的信息根据其敏感程度采取相应的保护措施。

8.3.6 合规自评估

合规自评估是指网络安全运维过程中,对需求方在国家法律法规、政策、标准规范以及区域、行业的网络安全监管要求中识别、分析组织安全合规需求,定期开展安全合规检查或检测,明确现有安全保障措施与安全监管要求差距,在此基础上进行合规建设,确保组织始终满足国家、区域、行业监管要求。网络安全运维工作中的安全合规工作是提供方与需求方共同完成的自评估工作,其主要工作内容包括:

- a) 评估检测:依据国家法律法规、政策、标准规范以及区域、行业的网络安全监管要求,对安全现状进行自查或配合安全测评机构/上级监管机构开展合规检查,查找不符合项,出具安全合规自评估报告;
- b) 合规整改建设:根据安全合规自评估报告,制定安全合规建设方案,进行合规整改,并针对建设整改结果开展自评估复测。

8.4 防护

8.4.1 概述

通过设备安全运维、安全加固、数据安全防护、密码应用安全等活动,实现网络安全运维的纵深保护。

8.4.2 设备安全运维

设备运维主要是对组织内的各种信息技术设备进行全面、细致、有效的日常维护和管理,以确保其正常运行并能够及时应对各种安全威胁。设备安全运维内容包括如下。

- a) 可用性监控:实时监控设备的运行状态和性能指标,及时发现和处理设备故障或异常情况,确保设备的可用性和可靠性。
- b) 设备更新和升级:根据组织机构的安全需求和设备厂商的建议,及时更新和升级设备,以提高设备的防护能力和安全性。
- c) 安全策略管理:根据业务及安全需求,调整和修改设备安全策略,并对策略进行归并及优化。
- d) 安全配置管理:定期梳理检查设备的配置,如访问控制配置等。对配置文件定期进行备份,并将备份文件存储在安全可靠的位置;同时,测试配置恢复功能,确保在需要时能够快速恢复设备配置。
- e) 设备的审计和记录:对设备的操作进行审计和记录,包括设备的配置操作、检测和监控操作、故障处理操作等,确保设备的操作合规性和可追溯性。
- f) 设备安全性管理:建立设备安全管理制度,对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期、维修过程等方面作出规定;根据运行参数研判、预测设备故障运行隐患、安全设备的告警进行及时分析和研判;定期开展安全设备漏洞排查,经过充分测试评估后,对已有漏洞及时修补。
- g) 安全有效性验证:结合安全运维实际工作的情况,对相关安全措施的有效性进行验证,以确保安全运维工作收到预期的效果。

8.4.3 安全加固

安全加固主要是针对网络与应用系统的加固,在网络设备、安全设备、操作系统、硬件设备、应用程序等层次上建立符合安全需求的安全状态。根据专业安全评估结果,制定相应的系统加固方案,针对不同目标系统实施不同策略的安全加固,例如打补丁、修改安全配置、增加安全机制等方法,合理进行安全性加强,从而保障信息系统的安全。安全加固内容包括如下。

- a) 安全现状调查:了解资产安全现状和资产关联关系,评估安全缺陷或安全隐患的影响范围和严重程度。
- b) 制定加固方案:针对发现的安全现状问题,督促指导或协同相关业务部门、建设部门、管理部门、运维部门等联合确认安全加固方案,包括实施时间、范围、流程、方法等,确认每项加固措施和操作方法的可行性,同步制定回退方案和应急方案。
- c) 落实加固举措:督促指导或协同资产责任人完成安全加固工作,安全加固前做数据备份、版本备份,分阶段、分批次有序开展安全加固举措、测试验证;针对重要资产,先加固资产,测试无误后再小批量、分批次开展安全加固。
- d) 验证加固结果:通过测试、攻击等手段,针对安全加固后的结论进行验证,根据验证结果判断是否符合加固要求,最终按需落实加固方案。

8.4.4 数据安全防护

通过数据加密、访问控制、数据备份和恢复、安全审计、监控、防护有效性评估等多种安全技术和策略,保护企业的敏感数据免受未经授权的访问、泄露、篡改和破坏。网络安全运维涉及的数据安全防护环节包括:

- a) 数据保护需求调查:了解数据安全现状,评估数据安全隐患,明确数据保护需求;
- b) 制定数据安全保护方案:针对发现的数据安全问题及需求,与数据管理部门、业务部门等制定数据安全保护方案;
- c) 按照 GB/T 45577 开展数据安全风险评估;
- d) 开展数据全生命周期安全保护:采取数据采集验证、数据传输加密、数据存储加密、数据访问控制、最小权限配置、数据脱敏、数据交换保护、数据备份和恢复、数据安全审计、数据安全监控、数据销毁管理等多种安全技术和策略,保护企业的敏感数据免受未经授权的访问、泄露、篡改和破坏;
- e) 数据安全防护措施有效性验证:定期对网络数据、终端数据等数据防泄露保护机制及有效性进行安全性评估和验证。

8.4.5 密码应用安全

落实信息系统密码应用安全。在信息系统物理环境、网络通信技术、设备、应用和数据等涉及密码应用的技术层面和人员管理、系统建设运行等涉及密码应用的管理层面,按照 GB/T 39786 相应级别落实密码应用安全要求。

8.5 监测分析

8.5.1 概述

通过网络流量监测、互联网资产暴露面监测、终端监测、数据监测、域名安全监测、实时分析和深度分析等威胁监测领域的活动,实现网络安全运维的实时威胁监测。

8.5.2 网络流量监测

网络流量监测是通过对进出网络的流量进行采集和分析,识别出存在的安全威胁。网络流量监测内容包括:

- a) 流量采集:通过部署网络监测设备,监测网络边界、网络出入口等关键节点的流量信息,发现网络攻击和存在的安全风险;
- b) 流量分析:可采用多种技术进行网络流量和威胁监测,基于规则库和威胁信息,采用特征匹配、网络行为分析、机器学习、关联分析等方法对采集的流量数据进行分析;
- c) APT 攻击监测:监测 APT 组织对重点单位的网络安全攻击,包括检测 APT 组织活动和事件、检测 APT 攻击链、检测未知 APT 事件等;
- d) 流量存储:明确采集的流量范围和类别,对监测流量采取保护措施,防止其受到未授权的访问、修改和删除,原始流量按照法规留存时间要求进行存放和归档。

8.5.3 网络资产暴露面监测

资产暴露面监测是通过网络空间测绘、资产管理、脆弱性管理等技术手段对网络出入口地址、信息系统(网站、APP、公众号、小程序等)、网络类设备、终端等进行监测,发现存在的可用性问题及安全威胁,根据监测结果采取相关举措抑制或控制事态影响。网络资产暴露面监测内容包括:

- a) 资产监测:结合网络主动扫描、流量被动还原、终端指纹采集、数据导入等方式,对合规资产、未纳管资产、隐匿资产等资产信息进行发现和持续监测,实现信息系统资产管理的全面覆盖,并将采集到数据汇聚成一份完整的资产清单;
- b) 漏洞监测:通过漏洞扫描工具等技术手段对信息系统及其支撑软硬件系统存在的漏洞进行发现和监测,对漏洞影响范围进行统计分析;
- c) 暴露面管理:关闭非必要网络协议地址、端口、应用服务等,收敛网络出口数量,减少对外暴露组织架构、邮箱账号、组织通信录等内部信息,避免在代码托管平台、文库、网盘等公共存储空间存储网络拓扑图、源代码、网络协议地址规划等可能被攻击者利用的技术文档。

8.5.4 终端监测

终端监测是通过对终端行为进行持续监测,实时收集并提取终端的威胁信息和行为数据,结合多种异常行为分析建模工具,发现存在风险的设备并进行及时响应,防范来自终端的安全威胁。终端监测内容包括:

- a) 终端数据采集:通过技术手段采集终端数据,主要包含服务、进程、端口、注册表、计划任务等;
- b) 终端威胁监测:通过终端威胁检测技术对终端进行监测,包含恶意代码检测、暴力破解检测、流量攻击检测、异常行为检测等;
- c) 终端监测技术:基于多种技术进行终端威胁检测,包括 IOA 行为检测、IOC 特征匹配、机器学习、关联分析、威胁图谱等。

8.5.5 数据监测

数据监测是通过数据库审计、数据防泄露等技术手段对数据采集、存储、传输、使用等过程进行监控,及时发现并阻断对数据进行的窃取、篡改和销毁等恶意行为。数据监测内容包括:

- a) 数据库监测:通过对数据库运行状态和操作行为进行监测,及时发现数据库的异常状态和异常操作行为等并定位问题;

- b) 管理策略监测:对数据管理策略落实情况进行监测,确保数据的保密性、完整性符合管理要求,保障数据传输、存储和使用的安全;
- c) 敏感数据监测:对敏感数据流转情况进行监测,及时发现和处置数据泄露威胁;
- d) 监测信息保存:对监测信息采取保护措施,防止其受到未授权的访问、修改和删除,监测信息的保存按照法规留存时间要求进行存放和归档。

8.5.6 域名安全监测

域名安全监测是通过监控企业关键域名服务,发现 DDOS 攻击、域名恶意解析等异常情况,防止隐蔽的网络攻击威胁。域名系统监测服务内容包括:

- a) 域名监测:监测域名地址记录(A 记录)、CNAME 等解析记录,发现解析异常;
- b) DNS 解析与监测:通过提供 DNS 解析服务或分光的方式,获取网络内 DNS 流量,通过重组和还原后在此基础上进行 DNS 请求/响应的监测和阻断。

8.5.7 实时分析

实时分析是通过统一采集终端业务数据与边界网络安全设备的海量日志,经实时流式大数据处理引擎对数据进行实时的归一化适配处理,处理后的数据通过关联规则引擎、异常流量行为引擎、AI 算法引擎等手段,运用机器学习、统计分析、构建基线等方法,从而发现网络中潜藏的网络攻击。实时分析服务内容包括:

- a) 实时资产监测:通过采集系统、应用日志和系统网络流量的状态或可疑活动,对资产健康情况进行实时监测;
- b) 异常行为监测:依靠已知特征、已知行为模式形成的攻击特征库,结合云端威胁信息,通过预定义规则、信息匹配等方式进行异常行为监测和安全处置;
- c) 实时关联分析:对多源安全日志进行实时关联分析,包括关联匹配、统计分析、时序分析、场景化模型、AI 引擎等;
- d) 事件数据保留:通过收集和集中存储在安全监测和分析过程中所有的事件,按照法规留存时间要求进行存放和归档;
- e) 警报和警告:通过安全设备告警日志、安全公告和漏洞信息、可扩散的威胁告警匹配所关注的信息资产,分析其所面临的潜在风险,第一时间发布事件预警通报;
- f) 数据分析和查询:对处置报告中有关分析数据和报告所需查询数据做出实时响应支持。

8.5.8 深度分析

深度分析是通过使用数字取证和恶意软件分析等技术手段,调查受影响的系统、审查受损的数据,还原攻击源头、攻击过程、攻击影响范围,形成证据链,并分析攻击中使用的工具和方法。深度分析的内容包括:

- a) 证据收集:收集和保存与所评估安全事件相关的数字证据,保管证据链,确定和维持证据的有效性;
- b) 溯源分析:通过对内部和外部攻击者的属性进行跟踪和追踪,提升其攻击溯源能力,形成攻击者画像,根据其跟踪和追踪结果,结合安全防护技术手段以减少安全事件发生概率;
- c) 取证分析:通过对与安全事件有关的数字证据的分析,以确定事件发生原因和过程;
- d) 未知威胁分析:结合静态检测、动态检测和沙箱检测等方式,对每个取证过程中发现的攻击者部署的恶意软件、程序或脚本进行分析,识别未知恶意代码和未知高级攻击行为。

8.6 事件处置

8.6.1 概述

事件处置包括建立应急预案、应急响应、处置与恢复、事件总结等活动。

8.6.2 应急预案

通过制定应急预案以提高应对网络安全事件的能力,预防和减少网络安全事件造成的损失和危害。应急预案基于组织的需求和特定情况,包括对可能发生的紧急情况进行风险评估和针对性的预防措施,包括以下内容。

- a) 按照 GB/T 24363 的步骤和关键要素制定应急预案。
- b) 网络安全应急预案基本内容包括:明确应急组织与人员、事件分类分级、应急处置方案、应急资源分配、通信策略、应急演练计划等关键要素。
- c) 网络安全运维过程中常用网络安全应急预案类型包括:
 - 1) 综合应急预案:应急预案是从总体上阐述事故的应急方针、政策,应急组织结构及相关应急职责,应急行动、措施和保障等基本要求和程序,应对各类信息安全事件的综合性文件;
 - 2) 专项应急预案:针对具体的事故类别、级别、应急保障而制定的计划或方案,是综合应急预案的组成部分,按照应急预案的程序和要求组织制定,并作为综合应急预案的附件,明确程序和具体的应急措施;
 - 3) 现场处置预案:现场处置预案是针对具体的场所、设施、岗位所制定的应急处置措施,现场处置方案宜具体、简单、针对性强,现场处置方案需结合现场脆弱性控制措施进行制定。
- d) 定期演练:确保员工和相关部门了解应急程序,熟练应对各种紧急情况,定期按照应急演练计划,进行实际的或模拟的演练和演习。
- e) 对应急预案进行版本控制,定期审查、更新和维护,确保预案的适应性和有效性。

8.6.3 应急响应

应急响应内容包括如下。

- a) 事件识别和报告:建立有效的事件识别机制,以及与员工和利益相关者进行有效沟通的渠道,根据事件现场威胁分析和按照 GB/T 20986—2023 第 5 章和第 6 章规定,判断事件类型与级别,对 GB/T 20986 规定的三级以上安全事件及时报告并触发应急响应程序。
- b) 应急响应启动:现场处置人员和相关技术人员第一时间根据事件发生情况,初步判断事件类型,并根据应急预案确定是否启动应急响应,并按照 GB/T 20985.2 确定是否启动事件响应。
- c) 事件分析和系统恢复:在网络安全事件发生后进行事件分析,确定存在的安全漏洞并采取必要的措施来修复漏洞,以防止类似事件的再次发生;在分析完成后,将被破坏的系统进行恢复,确保系统的完整性和可用性。
- d) 溯源取证:遵循法律程序和技术规范,完成攻击事件的溯源,确保取证数据的真实性和完整性,为后续的事件响应和安全分析提供支持。

8.6.4 处置与恢复

处置与恢复内容包括:

- a) 事件处置:在判断事件类型可能为安全事件,启用应急响应后,按照 GB/T 20986 的要求判断事件类型与级别,技术人员通过现场或非现场等方式进行信息收集工作,详细了解掌握事件发

生的始终、现状、可能的影响,进行详细分析后提供事件处置建议;

- b) 恢复:定期进行备份及数据恢复测试,保障存储位置的安全性。按照 GB/T 28827.3 的要求,督促指导或协同业务部门及应用系统建设运维部门,基于应急响应预案、配置管理数据库、知识库等进行故障处理和系统恢复,在满足事件级别处置时间要求的前提下尽快恢复服务,采用方法、手段防止次生、衍生事件的发生;
- c) 事件归档:事件处置结束,输出样本文件和事件处置报告,进行事件归档。

8.6.5 事件总结

事件总结包括如下内容。

- a) 事件处置分析:事件处置结束后,整理事件分析、处理的过程记录和相关资料,撰写应急响应记录报告并提交。对于大型、复杂的事件响应过程还应进行关联性事件处置汇报工作,同时,依据现场情况,召集必要相关人员发起会议,对本次事件的发生和处置过程进行总结,提升优化效率,优化运维方案,同步完善安全管理制度和流程。
- b) 工作总结:组织定期对事件响应工作进行分析和回顾,总结经验教训,并采取适当的后续措施。对事件响应工作的分析和回顾应形成总结报告,并将总结报告作为改进事件响应工作及信息系统的重要依据。
- c) 工作评审:为保证事件响应的有效性和时效性,事件响应责任者定期组织对事件响应工作的评审,以确保事件响应过程和管理符合预定的要求,评审的结果应正式存档并通知给相关利益方。评审至少每年举行一次。
- d) 工作改进:事件总结、工作评审的结果应作为准备阶段各项工作的改进要素,组织根据总结报告中给出的建议项和评审结果,完善安全运维应急准备工作,根据需要进行应急预案的修订和更新。

8.7 协同

8.7.1 概述

在网络安全运维体系化建设过程中,应开展人员能力提升、供应链安全管理、信息协同共享等与多方机构协同完成的基础性和提升性工作。

8.7.2 人员能力提升

人员能力提升内容可包括:

- a) 理论知识培训:对专业技术人员提供专项提升培训和考核,掌握前沿技术、产品应用等内容,提升相关人员技术知识水平;
- b) 安全意识宣传:通过视频、海报、易拉宝、月刊、手册、电脑桌面等形式,对全体员工进行安全意识的宣传和教育,形成网络安全宣传教育常态化机制;
- c) 专业技能演练:通过渗透测试、攻防演练、技能比赛等有限定的网络攻击演练,加深运维人员对网络攻击实操的认知,熟悉系统风险和应对措施,提升技术人员网络攻击防范能力。

8.7.3 供应链安全

建立供应链安全控制策略及机制,在网络安全运维过程中实施全过程安全管理,避免由于供应链环节的安全隐患,导致恶意代码植入、挟持、信息泄露、钓鱼攻击和远程控制等安全问题。安全运维团队督促指导或协同供应链相关单位达到供应链安全要求。供应链安全相关的实施内容包括:

- a) 供应商管理:组织建立供应商等级评价及准入、准出机制,通过充分的审核和评估,确保供应商安全能力持续符合要求组织,按照 GB/T 43698—2024 中 7.1.4 的要求,建立供应商替代方案或具备相应软硬件系统的自主维护能力,防范供应链中断风险;
- b) 安全协议:确定供应商及内部组织在供应链安全管理中的责任,结合业务特点和等级明确供应商的服务保障要求,明确与供应商发生业务关系时的安全性要求。与供应商签订的协议包含 SLA 的相关内容,确保供应商的服务保障,并定期评估协议的有效性;
- c) 安全监测:在运维过程中对供应链安全态势进行监测;建立监控机制以及时发现并上报存在的风险和问题;
- d) 安全响应:建立供应商安全响应机制,以确保在发生安全事态或事件时,供应商能够积极配合响应,至正式关闭;若必要,供应商应进行事后分析,确定起因;
- e) 绩效管理:组织按计划的时间间隔监督供应商的安全绩效,如未达成绩效目标或未履行协议义务的,应确保及时识别改进机会,并制定相应措施;
- f) 风险管理:结合组织业务特点,识别和梳理供应链面临的风险,分析风险发生概率,评估影响范围和程度,制定相应措施或预案以控制风险,并针对供应链关键环节,实施风险评估审查。

8.7.4 信息协同共享

信息协调共享内容包括:

- a) 信息收集:组织持续关注、抓取、汇总、甄别、整理获取到的安全相关信息,并结合研究成果,形成安全通报或专题报告等信息文档;
- b) 信息共享:组织建立信息共享渠道,明确信息共享流程,定期组织沟通、交流,保障组织间的信息同步;
- c) 协同响应:组织明确共同目标,建立协同机制,实现跨组织合作,以更好地利用外部资源提升效率。

8.8 运维效果评估

8.8.1 效果评估内容

8.8.1.1 概述

效果评估的核心目标是通过量化和分析,确保安全措施的有效实施,并为持续改进提供依据。宜参考 GB/T 31495.2,从建设、运行、态势三个角度设定指标,评估安全运维效果。

8.8.1.2 建设效果评估

评估各项安全运维要素是否建立,宜考虑如下因素:

- a) 流程建立的全面性和规范性,实际建立的流程数量占应建立流程的比例;
- b) 工具类型和功能对安全运维工具需求的覆盖度;
- c) 人员团队的职责、规模、资质与安全运维团队需求的匹配度,团队实际人员数量占应配置的人员规模的比例。

8.8.1.3 运行效果评估

评估各项安全运维措施执行结果是否达到了预期的目标值,宜考虑如下因素:

- a) 流程执行过程的及时性,如平均事件检测时间(MTTD)当前的测量值和设定的目标值之间的差距;

- b) 流程执行结果的完成度,如工单完成率、资产信息完整登记率等测量结果和预期目标值的差距;
- c) 工具部署范围的全面性,如终端安全软件安装率、流量分析覆盖率;
- d) 工具安全功能的有效性,如规则告警准确率、攻击拦截率;
- e) 人员安全技术和意识水平,如培训出勤率、考核合格率。

在开展运行效果评估过程中,数据采集工作应持续关注其自动化能力以及数据采集的收益与成本的对比情况,并在持续运营过程中不断提升数据采集的自动化能力。

8.8.1.4 安全态势评估

评估开展安全运维后实际的安全保障结果,宜考虑如下因素:

- a) 发生安全事件的次数与严重性;
- b) 出现脆弱性的次数与严重性。

8.8.2 评估过程

网络安全运维需求方与提供方定期对安全运维效果预期目标进行审查,根据安全运维需求选取合理的评估范围,每年可组织一次安全运维效果评估,发生重大变更时重新进行评估,以保证网络安全运维工作有效性。评估过程宜遵循以下原则:

- a) 科学性:按照网络安全运维效果评估指标框架,选择科学的评估方法;
- b) 公正性:网络安全运维效果评估过程符合法规和组织原则,保证评估结果是客观公正准确的;
- c) 安全性:向网络安全运维需求方告知评估时间、评估工具、评估技术方式以及可能对信息系统造成的影响等,确保评估活动自身安全性;
- d) 受控性:有外部人员参与评估的情况下,相关人员签署保密协议,若需提供实际数据进行评估参考,进行脱敏处理,并对评估过程数据和结果数据进行严格管理;
- e) 计划性:开展评估前制定评估计划,明确评估目标、范围、时间、方法和预期结果,由运维需求方和运维提供方达成共识;
- f) 透明性:网络安全运维提供方按评估目标提供必要的过程数据(包括但不限于安全漏洞评估报告、安全防护有效性验证报告、安全监测操作记录等),确保评估结果的准确透明。

8.8.3 评估方法

8.8.3.1 方法选择

安全运维效果评估可根据评估场景选择具体的评估方法,包括顾问访谈、问卷调查、文件审核、勘查调研、漏洞扫描、渗透测试、红蓝对抗、技术验证等多种评估方法可根据实际场景搭配使用。评估方法包括:

- a) 顾问访谈:顾问访谈是通过与安全专家或顾问进行面对面或远程对话,以了解系统安全性和潜在风险的方法,适用于包括提问有关安全人员组织、管理策略与制度、系统配置和实施相关的评估指标;
- b) 问卷调查:问卷调查是一种通过向相关人员发送一系列安全问题或调查表,以便收集他们的观点和反馈的方法,适用于人员安全意识和安全实践情况相关的评估指标;
- c) 文件审核:文件审核涉及检查系统、应用程序或网络的相关文件和文档,如安全策略、配置文件和日志记录,有助于发现潜在的安全问题和不符合安全要求的情况,适用于安全人员组织、管理策略与制度、系统配置和实施相关的评估指标;

- d) 勘查调研:通过实地勘查或远程调查,了解物理设备、网络拓扑和环境因素对安全性的影响。适用于物理安全相关的评估指标;
- e) 漏洞扫描:使用自动化工具来识别系统或应用程序中的已知漏洞和弱点,适用于技术性相关的评估指标以及对组织已部署的各类安全产品和规则策略开展技术验证;
- f) 渗透测试:渗透测试人员模拟攻击者的行为尝试入侵系统,发现潜在漏洞但不会造成破坏,并提供详细的报告和建议,以加强安全,适用于技术性相关的评估指标,以及对组织已部署的各类安全产品和规则策略开展技术验证;
- g) 红蓝对抗:红蓝对抗是一种模拟攻击和防御的综合性安全测试方法。红蓝两队在模拟环境中对抗,以评估系统的安全性和响应能力,适用于技术性相关的评估指标,以及对组织已部署的各类安全产品和规则策略开展技术验证。

8.8.3.2 汇总评分

安全运维效果汇总评分用于量化评价、考核安全运维工作的实际效果。组织可按照安全运维需求和目标,选取建设指标、运行指标和态势指标及目标值,确定各指标类别权重,形成评估基线。各指标项根据其测量结果与目标值的差值进行评分,并按照权重转化为百分制,实现安全运维效果的量化考核。

8.8.4 持续改进

安全运维效果评估后持续跟踪改进。安全运维需求方和提供方应共同分析评估结果,制定改进计划并持续跟踪,解决评估中发现的问题和风险。持续改进措施包括:

- a) 网络安全运维效果的评估融入日常的运维工作中,形成持续性的监控和评估机制;
- b) 明确具体部门及人员参与网络安全运维的整改建议计划、所需资源,及其形成的任务(项目);
- c) 确定实施改进任务计划的时间安排和任务分配,包括评估后的具体安排节点以及重要里程碑节点;
- d) 确定对网络安全运维的效果提升结果和整改任务的实施情况进行监控的措施;
- e) 及时发现正在整改过程中产生的新风险或已知风险随着环境和时间发生的变化,以及持续进行评估;
- f) 按照预定的时间和任务安排跟进整改进度,完成整改任务的验收总结和复审。

附录 A
(资料性)
网络安全运维能力评估

A.1 评估模型

网络安全运维的能力评估模型内容包括以下几个方面：

- a) 网络安全运维实施内容：主要针对与网络运维实施活动直接相关的识别、防护、监测分析、事件处置等环节；
- b) 网络安全运维关键要素：明确组织机构在整个安全领域中所具备的关键要素，明确为安全运维团队、安全运维工具和平台以及安全运维的各类流程；
- c) 网络安全运维级别：可基于统一的评估模型，定义组织在网络安全运维域的能力级别。

网络安全运维能力评估模型如图 A.1 所示。

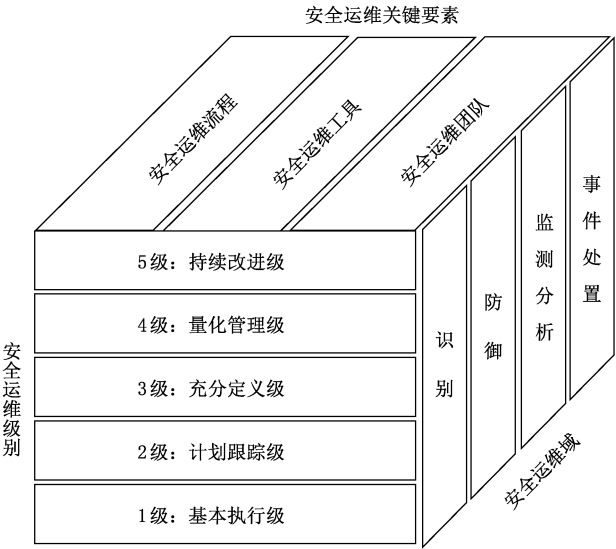


图 A.1 网络安全运维能力评估模型

安全运维能力级别可分为五个等级，一级是基本执行级，二级是计划跟踪级，三级是充分定义级，四级是量化控制级，五级是持续改进级。运维能力等级从一级至五级逐级提升。对运维能力等级的描述如表 A.1 所示。

表 A.1 网络安全运维能力等级

运维能力级别	定义内容	执行表现	特征
等级一：基本执行级	<ul style="list-style-type: none">● 未形成成熟的机制保证安全运维工作的有序开展● 安全运维工作处于被动执行阶段	执行力较差，资源、能力严重不足	以边界防护为核心

表 A.1 网络安全运维能力等级（续）

运维能力级别	定义内容	执行表现	特征
等级二：计划跟踪级	<ul style="list-style-type: none"> 工作有计划并可执行，对安全运维过程进行了规划，提前分配资源和责任 按照预定的方式执行并能通过结果进行跟踪和纠偏 	实现了安全过程的计划与执行，不成体系	以技术产品部署为核心的基础防范
等级三：充分定义级	<ul style="list-style-type: none"> 有标准化的制度和流程，有清晰的标准化文档支撑安全运维各项目 形成业务系统内、各业务系统之间、组织机构外部活动的协调机制 	执行效果较好，但有较大改进空间	以合规体系建设为核心的体系化控制
等级四：量化控制级	<ul style="list-style-type: none"> 有清晰可测的网络安全运维指标，安全运维内容可量化 通过量化测量来管理安全运维的全过程，并可修正安全运维相关行动 	执行效果非常好，改进空间较小	以攻防对抗为核心的主动防御
等级五：持续改进级	<ul style="list-style-type: none"> 形成了内生的安全循环机制并不断演化 防护能力和人员能力不断提升 	执行效果非常好，人员的信息安全意识很强，形成信息安全文化	

A.2 评估内容

A.2.1 网络安全运维的实施内容评估

网络安全运维的实施内容评估主要针对识别、防护、监测分析和事件处置四个环节的活动，评估内容包括但不限于：

- 识别环节的评估内容包括业务识别、资产识别、风险识别、威胁信息收集与合规自评评估等内容；
- 防护环节的评估内容包括设备安全运维、安全加固、数据安全防护和密码应用安全等内容；
- 监测分析环节的评估内容包括网络流量监测、网络资产暴露面监测、终端监测、数据监测、域名安全监测、实时分析、深度分析等内容；
- 事件处置环节的评估内容包括应急预案、应急响应、处置与恢复、事件总结等内容。

A.2.2 安全运维关键要素评估

网络安全运维关键要素相关的评估以下方面。

- 从承担安全运维工作的组织机构建设具备的能力出发，从以下方面对安全运维团队进行评估：
 - 安全运维组织架构对组织业务的适用性；
 - 安全运维组织机构承担的工作职责的明确性、人员能力的匹配性；
 - 安全运维组织机构运作、沟通协调的有效性。
- 约定和规范日常安全运维工作中各操作环节、操作步骤、操作工具、操作方法，以维持工作进程的一致性和统一性，实现精细化、标准化的安全运维管理，提升工作效率，从以下方面对安全运维流程进行评估：
 - 安全运维活动中关键控制节点授权审批流程的完整性；

- 2) 相关流程制度的制定、发布、修订的规范性和专业性；
- 3) 安全要求及流程落地执行的一致性、有效性和体系化。
- c) 从安全运维组织用于开展工作的安全技术、应用系统和自动化工具出发,从以下方面对安全运维工具进行评估:
 - 1) 从网络侧、主机侧、应用侧、策略侧、终端侧和账号侧等多个维度获取多源数据的能力；
 - 2) 对比历史数据,形成趋势性、合理性判断,实现全方位、多层次、多角度、细粒度感知,为安全运维提供重要分析能力；
 - 3) 将团队、流程、工具有机结合以实现自动化、数据化、智能化的业务流转、业务监控和业务考核,快速提升和持续改进安全能力。

A.3 评级方法

安全运维评级用于定性评价组织整体网络安全运维能力,指导组织长期的安全运维规划与建设。

组织可按照安全运维能力评估模型设定能力评估指标,针对特定安全运维内容评估各项指标的满足情况。仅在符合某一级别全部指标的情况下,认定组织机构达到该级别能力要求,由低到高以此类推可测得最终能力级别。实际评估中,根据组织安全运维情况剔除不涉及的指标。



附 录 B
(资料性)
网络安全运营中心建设

B.1 建设模式**B.1.1 总则**

网络安全运营中心建设模式包括全自建、联合和全托管三种模式,组织根据安全要求、运维资源投入和安全运维能力决定采用哪种模式。当组织对网络安全和数据保护的要求非常高,有足够的安全资源投入,且自身安全运维能力强时,可选择全自建模式;当组织对安全性和数据保护的要求较高,有较充足的安全资源投入,自身安全运维能力较强时,可选择联合模式;当组织对安全性和数据保护的要求不高,有一定的安全资源投入,自身安全运维能力不强时,宜选择全托管模式。三种模式的网络安全运营中心在安全运维人员与岗位职责、安全运维管理流程上存在不同。一般情况下,三种模式的网络安全运营中心均设置两类工作岗位,分别是管理类和技术类,其中技术类又分为分析研判和实施操作两类。

B.1.2 全自建网络安全运维**B.1.2.1 岗位职责****B.1.2.1.1 管理类**

全自建模式下的管理类主要包括安全运营中心负责人、安全运维主管、安全技术主管、安全监测主管和风险与合规管理岗。管理类职责包括:

- a) SOC 负责人:主要工作包括负责组织制定安全运维目标和工作计划、安全运维能力规划和建设、安全运维制度和流程,跟踪监督执行效果,重大运维事项的决策等;
- b) 安全运维主管:向安全运营中心负责人汇报,主要工作包括负责落实安全运维目标、执行工作计划、优化改进安全运维制度和流程和落实重大运维事项决策等;
- c) 安全技术主管:安全运营中心负责人汇报,主要工作包括负责安全运营中心技术平台与工具整体架构体系设计及其建设规划、技术平台与工具选型上架、组织内技术标准制定、技术平台与工具定制开发与维护等;
- d) 安全监测主管:向安全运营中心负责人汇报,主要工作包括负责管理网络安全事件,突发事件的应急响应、调查分析和追踪溯源,安全事件的联动处置和网络安全态势报告的编制等;
- e) 风险与合规管理岗:向安全运营中心负责人汇报,主要工作包括对国家网络安全政策、标准宣贯;网络安全相关资质的获取和维护,确保参与安全运维人员符合相关保密性工作要求,负责网络安全风险全过程管理与网络安全合规管理等。

B.1.2.1.2 技术类

全自建模式下的技术类包括分析研判类和实施操作类。

- a) 分析研判类主要包括安全监测岗、分析研判岗、漏洞分析岗、威胁信息分析岗、防护策略分析岗、攻防对抗分析岗六类岗位:
 - 1) 安全监测岗:向安全监测主管汇报,主要工作包括负责相关设备的日志分析、策略调整、规则优化、威胁事件监测上报,执行和落实网络安全态势监测分析方案,处置突发事件,跟踪

安全事件整改情况；

- 2) 分析研判岗:向安全监测主管汇报,主要工作包括负责分析安全威胁告警报告、分析是否启动应急流程、网络安全威胁事件深入分析与溯源,分析和报告网络安全防御措施缺陷等;
 - 3) 漏洞分析岗:向安全监测主管汇报,主要工作包括负责安全漏洞跟踪分析评估、预警信息发布、漏洞修复方案和加固措施制定、漏洞处置过程监控、漏洞修复情况验证分析等;
 - 4) 威胁信息分析岗:向安全监测主管汇报,主要工作包括负责威胁信息的采集分析评估、获取数据的归类分析整合等;
 - 5) 防护策略管理分析岗:向安全监测主管汇报,主要工作包括负责安全防护策略的管理、优化、制定、执行和有效性分析等;
 - 6) 攻防对抗分析岗:向安全监测主管汇报。负责向驻场运维人员提供红蓝对抗演练、渗透测试、代码审计等攻防专家能力支持。
- b) 实施操作类主要包括安全响应岗、资产维护岗、平台维护岗、主机安全维护岗、终端安全维护岗、集权设备维护岗六类岗位:
- 1) 安全响应岗:向安全监测主管汇报,工作内容包括负责威胁信息事件响应、安全事件处置、应急响应等事件闭环等;
 - 2) 资产维护岗:向安全运维主管汇报,主要工作包括负责组织信息资产的发现、资产清单的管理、资产档案的维护、问题资产的发现和处置等;
 - 3) 平台维护岗:向安全运维主管汇报,主要工作包括负责安全设备与平台的定期升级更新、状态巡检、故障排除、设备与平台预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等;
 - 4) 主机安全维护岗:向安全运维主管汇报,主要工作包括负责主机服务器的定期升级更新、状态巡检、故障排除、主机服务器预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等;
 - 5) 终端安全维护岗:向安全运维主管汇报,主要工作包括负责终端设备的定期升级更新、状态巡检、故障排除、终端设备预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等;
 - 6) 集权设备维护岗:向安全运维主管汇报,主要工作包括负责集权设备的定期升级更新、状态巡检、故障排除、集权设备预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等。



B.1.2.2 管理流程

全自建网络安全运维管理流程主要优势是熟悉组织文化与业务、理解安全需求透彻,创建的流程贴合组织实际;劣势是对最佳实践和新技术理念了解滞后,对流程的优化和变革缺乏驱动力。全自建网络安全运营中心在网络安全运维流程管理包括如下。

- a) 识别流程:通过确定对象、收集数据、选择方法、分析规律、判断检查、建立模型和验证评估等环节完成;全自建网络安全运营中心宜按照 GB/T 20984,创建和管理业务识别流程、资产发现与管理流程、风险管理流程。业务识别流程包括业务发展战略和业务关联关系内容;资产发现与管理流程包括依据资产业务承载性确定资产重要性的内容,同时要结合最新的资产识别和管理平台设计流程;风险管理流程包括必要时引入外部机构进行风险评估的子流程。威胁信息收集/评估/预警流程和安全合规管理流程考虑引入外部机构的条件和时机。

- b) 防护流程:通过识别网络安全缺失和漏洞、评估危害和级别、分析防护措施、制定工作任务和实施步骤、考核和修正等环节完成,一般包括安全设备和应用运维流程、安全加固流程、数据安全防护流程等涵盖纵深防御领域的流程;全自建网络安全运营中心在创建防护流程时充分了解最佳实践,评估技术发展趋势,持续优化改进防护流程。
- c) 监测流程:通过数据采集和存储、分析与合成、告警和查询、检测和发现等环节完成,一般包括网络流量监测、网络资产暴露面监测、终端监测、数据监测、域名安全监测、实时分析、深度分析等涵盖威胁监测领域的流程;全自建网络安全运营中心关注外部网络安全热点事件,结合威胁信息,及时调整监测重点,必要时调整防护策略。
- d) 响应流程:在日常工作中遵循准备、诊断、抑制、根除、恢复和跟踪等应急响应流程,处置突发事件的过程中通过识别发现并报告威胁级别、详细信息综合分析研判、阻断封堵、固定证据、业务恢复、溯源分析、还原攻击、事件报送以及配合相关部门追踪溯源等环节完成,该领域一般包括应急预案编制、应急响应与处置、安全应急演练和内部异常行为响应等涵盖应急响应领域的流程;全自建网络安全运营中心在应急响应流程中在保证安全的前提下,引入外部专家力量的条件、时机及相关的协同与保障机制。
- e) 网络安全运维沟通机制建立:全自建网络安全运营中心建立内部沟通机制和外部沟通机制,内部沟通机制包括与上级部门或管理层的汇报机制、与业务部门的通报与协同机制、与行政管理保障与支撑机制等,外部沟通机制包括与国家主管机关和上级单位的信息上报机制、与下属单位的通报预警机制、与其他单位的信息共享机制、与专业机构的协同机制等。

B.1.3 联合网络安全运维

B.1.3.1 岗位职责

B.1.3.1.1 管理类

联合模式下主建单位一般为网络安全运维需求方,承担指挥决策、组织管理,资源调度及信息协调等职责,并担任管理岗角色。

联合模式下的管理类主要包括 SOC 负责人、安全运维主管、安全技术主管、安全监测主管、风险与合规管理岗五个岗位。管理类职责包括:

- a) SOC 负责人:安全运营中心负责人主要工作包括负责组织制定总体安全目标和工作计划、安全能力规划和建设、安全制度和流程的评审、跟踪监督执行效果,重大事项的决策等;
- b) 安全运维主管:与主建单位内部各团队沟通协调,向安全运营中心负责人汇报,主要工作包括负责安全运维领域总体安全目标的分解和对应各分计划的制定、安全运维人员组织和能力的规则与建设、安全运维领域的安全制度和 workflows 制定与落实等;
- c) 安全技术主管:向安全运营中心负责人汇报,主要工作包括负责安全运营中心技术平台与工具整体架构体系设计及其建设规划、技术平台与工具选型上架、组织内技术标准制定、技术平台与工具定制开发与维护等;
- d) 安全监测主管:向安全运营中心负责人汇报,主要工作包括负责管理网络安全事件,突发事件的应急响应、调查分析和追踪溯源,安全事件的联动处置和网络安全态势报告的编制等;
- e) 风险与合规管理主管:向安全运营中心负责人汇报,主要工作包括对国家网络安全政策、标准宣贯;确保参与安全运维人员符合相关保密性工作要求;负责组织风险合规管理体系的构建和推进、风险控制机制的建立和实施、网络安全相关资质的获取和维护,合规制度和流程的维护等。

B.1.3.1.2 技术类

联合模式下的技术类岗位分为分析研判和实施操作。

- a) 分析研判岗位一般由合作方担任,依据安全运维需求,以驻场或远程方式提供安全运维服务,主要包括项目经理岗、安全运维咨询岗、安全监测岗、分析研判岗、漏洞分析岗、威胁信息分析岗、防护策略分析岗、攻防对抗分析岗八个岗位:
 - 1) 项目经理岗:向安全运营中心负责人汇报,主要工作包括负责项目资源协调和赋能申请、负责项目情况及问题跟进、项目交付周期管理、项目定期汇报及项目验收工作;
 - 2) 安全运维咨询岗:向安全运营中心负责人汇报,主要工作包括负责网络安全运营中心流程制度设计、技术体系设计、人员组织架构设计及落地跟进,并参与指导改进优化;负责跟进整体运维成熟度度量,依照度量结果动态改良整体运维体系等;
 - 3) 安全监测岗:向项目经理岗汇报,主要工作包括负责相关设备的日志分析、策略调整、规则优化、威胁事件监测上报,执行和落实网络安全态势监测分析方案,处置突发事件,跟踪安全事件整改情况;
 - 4) 分析研判岗:向项目经理岗汇报,负责向驻场运维人员提供安全威胁告警分析研判专家能力、策略优化、自定义规则能力支持,向主建单位提供紧急漏洞、事件的威胁情报;
 - 5) 漏洞分析岗:向项目经理岗汇报,主要工作包括负责安全漏洞跟踪分析评估、预警信息发布、漏洞修复方案和加固措施制定、漏洞处置过程监控、漏洞修复情况验证分析等;
 - 6) 威胁信息分析岗:向项目经理岗汇报,主要工作包括负责威胁信息的采集分析评估、获取数据的归类分析整合等;
 - 7) 防护策略分析岗:向项目经理岗汇报,主要工作包括负责安全防护策略的管理、优化、制定、执行和有效性分析等;
 - 8) 攻防对抗分析岗:向项目经理岗汇报。负责向驻场运维人员提供红蓝对抗演练、渗透测试、代码审计等攻防专家能力支持。
- b) 实施操作类一般由主建单位承担,也可由合作单位承担,主要包括安全响应岗、资产维护岗、平台维护岗、主机安全运维岗、终端安全维护岗、集权设备维护岗六个岗位:
 - 1) 安全响应岗:向安全运维主管汇报,工作内容包括负责威胁信息事件响应、安全事件处置、应急响应等事件闭环等;
 - 2) 资产维护岗:向安全运维主管汇报,主要工作包括负责组织信息资产的发现、资产清单的管理、资产档案的维护、问题资产的发现和处置等;
 - 3) 平台维护岗:向安全运维主管汇报,主要工作包括负责安全设备与平台的定期升级更新、状态巡检、故障排除、设备与平台预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等;
 - 4) 主机安全运维岗:向安全运维主管汇报,主要工作包括负责主机服务器的定期升级更新、状态巡检、故障排除、主机服务器预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等;
 - 5) 终端安全维护岗:向安全运维主管汇报,主要工作包括负责终端设备的定期升级更新、状态巡检、故障排除、终端设备预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等;
 - 6) 集权设备维护岗:向安全运维主管汇报,主要工作包括负责集权设备的定期升级更新、状态巡检、故障排除、集权设备预置及自定义规则、策略、预案、脚本、知识的建设、维护及发布等;

布等。

B.1.3.2 管理流程

在联合网络安全运营中心模式中,为确保安全运维管理流程可切实落地,明确安全运维各项工作中主建单位和合作单位的分工界面,整体分工界面可为主建方负责决策管理、跨部门沟通、资源及信息协调相关工作;合作方负责专业技术能力交付、安全运维专家咨询、云端技术能力支持等工作。在安全运维各个管理流程中,主建单位和合作单位分工界面如下。

- a) 识别流程:包含业务识别、资产识别、风险识别、信息收集、合规自评估等识别领域的流程,工作流程一般由信息收集、信息确认、确认反馈、信息梳理、信息消费等环节组成,其中信息确认及确认反馈环节由主建单位主责,信息收集、信息梳理及信息消费由合作单位主责。
- b) 防护流程:包含安全设备运维、安全加固、数据安全防护等领域的流程。工作流程一般由安全运维需求提出、安全服务/工具清单提供、安全服务/工具确定、安全服务/工具实施、服务/工具实施成果验收等环节组成,其中安全运维需求提出、安全服务/工具确定及服务/工具实施成果验收环节由主建单位主责,安全服务/工具清单提供、安全服务/工具实施环节由合作单位主责。
- c) 监测流程:包含网络流量监测、网络资产暴露面监测、终端监测、数据监测、域名安全监测、实时分析、深度分析等监测领域的流程。工作流程一般由监测范围覆盖、监测实施、分析实施、结果上报等环节组成,其中监测范围覆盖由主建单位主责,监测实施、分析实施、结果上报等环节由合作单位主责。
- d) 响应流程:包含应急预案、应急响应、处置与恢复、事件总结等领域的流程。工作流程一般由准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、总结阶段等环节组成,其中抑制阶段、恢复阶段、总结阶段由主建单位主责,准备阶段、检测阶段、根除阶段由合作单位主责。
- e) 建立安全运维协同机制:在联合网络安全运营中心模式中,为确保信息传递畅通,工作协同高效,建立安全运维协同机制:
 - 1) 接口人机制由信息安全管理领导和合作单位指定主建单位和合作单位接口人,合作单位接口人一般由项目经理担任。确保项目信息准确有效同步,并能统一归口;
 - 2) 云地协同机制由合作单位提供覆盖安全运维工作能力需求的云端专家能力团队,并针对云端威胁信息预警、云端 SaaS 化能力、地端协调指挥能力等云地协同工作提供便捷可靠的协同工具。

B.1.4 全托管网络安全运维

B.1.4.1 岗位职责

B.1.4.1.1 管理类

全托管模式下的运维管理类主要包括 SOC 负责人、安全运维主管、质量管理专家、风险与合规管理岗四个岗位,其中 SOC 负责人由网络安全运维需求方担任,其他管理岗可由被委托的服务单位担任,并向 SOC 负责人汇报。管理类职责包括:

- a) SOC 负责人:负责安全运营中心的领导工作以及重大事项的决策,能组织制定安全运维的发展目标和规划、指导制定安全运维的制度和流程,并跟踪监督执行效果;
- b) 安全运维主管:负责安全托管项目实施的监察、协调等管理工作,能帮助用户识别和确定网络安全需求、与甲方用户就共同安全目标进行沟通与协调,能组织建立和运行应急体系,能协调

内、外部相关方进行高等级网络安全威胁事件联动处置工作；

- c) 质量管理专家：负责安全托管整体质量管理、用户满意度管理，能制定质量要求及客户满意度要求，能及时进行质量审查及审查结果汇报，能对运维过程进行质量改进管理；
- d) 风险与合规管理岗：负责项目风险管理，对项目方案的风险进行识别和评估，能够依据相关法律法规、标准要求，结合实际业务需求和项目情况，提供合规咨询，进行风险分析并提供解决方案；确保参与安全运维人员符合相关保密性工作要求，进行合规监管、项目风险管控及评估。

B.1.4.1.2 技术类

全托管模式下的技术类分为分析研判和实施操作，由被委托的服务单位担任，依据安全运维需求，一般以远程的方式提供安全运维服务。

- a) 分析研判包括安全监测岗、分析研判岗、漏洞分析岗、威胁信息分析岗、防护策略分析岗等五个岗位：
 - 1) 安全监测岗：负责常态化安全监控工作，负责提供远程技术支撑、远程威胁分析、远程响应处置、定期对安全事件进行统计和报告等，能使用各类方法和工具对安全设备日志和流量等安全数据进行云端监控和分析，能规划设计安全监测分析方案，给出网络安全态势的合理评价；
 - 2) 分析研判岗：负责对各类安全事件进行研判分析，能够快速准确地进行事件确认、定级、问题定位、溯源分析，并提供可靠的遏制和恢复方案，能针对新型威胁进行深度分析、支持高级别攻击的分析和溯源，能开展运维自动化流程设计，帮助持续提升安全托管效果，为技术人员提供支撑；
 - 3) 漏洞分析岗：负责对最新安全漏洞进行跟踪、分析，能对漏洞和安全威胁进行评估，并制定适当的漏洞修复方案和加固措施；
 - 4) 威胁信息分析岗：负责云端威胁信息管理，能进行威胁信息源整合并沉淀为知识库，能够识别并应用适当的威胁信息与框架进行攻击者能力的跟踪与评估；
 - 5) 防护策略分析岗：负责安全防护策略的管理及优化工作，能够制定并执行安全策略并提供策略的有效性分析。
- b) 实施操作包括资产管理岗、安全运维岗、应急响应岗三个岗位：
 - 1) 资产管理岗：负责数据资产识别、脆弱性识别等工作，能针对企业业务现状制定数据资产梳理方案和数据分类分级实施准则，指导数据资产梳理工作的落地，并具备对网络安全资产安全风险等级分析与评估能力；
 - 2) 安全运维岗：负责运维管理工作部署、监控、优化、故障处理、周期性安全运维报告编制工作，具备安全隐患的排查分析能力，能对服务器、网络设备、安全产品、信息系统进行安全维护、安全巡检、策略维护管理、配置变更、故障处置与安全分析等，消除和降低所发现的威胁；
 - 3) 应急响应岗：负责制定安全事件应急响应预案，提供远程应急响应处置，能够对网络威胁和安全事件进行跟踪响应，能协同甲方团队进行事件处置和升级（远程/现场）。

B.1.4.2 管理流程

在全托管安全运维模式下，通过 SaaS 化的网络安全运营中心或远程接入本地网络安全运营中心，对用户侧的安全事件和相关数据源（包括日志、流量等）进行安全监控和威胁检测，并将各类监测结果以告警信息方式推送到网络安全运营中心/平台，自动生成处置工单后推送分配相应运维人员，对客

户的安全事件进行研判、排查和响应,形成“平台+流程+人”的安全托管服务。全托管网络安全运营中心建立以下流程。

- a) 识别流程:包括业务识别、资产识别、风险识别、威胁信息收集、合规自评估等子流程的创建。托管安全服务商与运维对象就安全运维目标达成一致,服务商对用户侧现网安全情况及相应业务流程现状进行调研,并根据调研结果进行设备部署接入、远程策略配置、测试和服务开通,由云端运维专家通过用户自主上报、安全工具扫描等主动或被动探测技术对用户资产、威胁信息进行全面识别与梳理,建立资产管理台账、威胁信息库等,并通过云端漏洞扫描、渗透测试等多种脆弱性评估手段及威胁发现方法,识别资产暴露面。
- b) 防护流程:包括安全设备运维、安全加固、数据安全防护等子流程的创建。托管安全服务商获取管理企业内部的特定安全工具的权限,通过识别安全隐患和漏洞、评估危害和级别、分析防护措施等一系列流程活动,提供安全加固措施及处置方案,并对用户安全设备和工具上的安全策略进行统一管理调整,确保安全策略保持处于最优水平。
- c) 监测流程:包括网络流量监测、网络资产暴露面监测、终端监测、数据监测、域名安全监测、实时分析、深度分析等子流程的创建。由托管安全服务商通过用户的本地收集器将原始日志、流量等数据传输到网络安全运营中心,持续分析监测网络安全状态,综合发现漏洞、弱口令、勒索等安全风险和异常行为,由云端安全分析人员对研判结果进行复核,在安全分析人员无法处置时,由安全专家对问题进行深入分析调查,获取授权后采取行动,借助本地或远程部署的相关安全工具完成查杀、封锁等处置流程,形成报告推送用户。
- d) 响应流程:包括应急预案、应急响应、处置与恢复、事件总结等子流程的创建。托管安全服务商遵循准备、诊断、抑制、根除、恢复和跟踪等应急响应流程,帮助用户在遭受突发事件后进行应急处理。通过识别发现并报告威胁级别、详细信息综合分析研判、阻断封堵、固定证据、业务恢复、溯源分析、还原攻击、事件报送以及配合公安部门追踪溯源等环节完成,同时定期复盘组织内的安全事件和风险情况,由托管安全服务商提供阶段性报告,并通过线上线下相结合的方式进行汇报,对重大事件复盘分析、总结经验,更新应急预案。
- e) 网络安全运维沟通机制建立:包括安全运维能力提升、信息协同共享、运维质量回访等子流程的创建。托管安全服务商及用户侧分别指定接口人(通常为项目经理),由服务商针对安全运维整体工作情况定期进行总结和汇报,并定期组织用户侧进行安全培训和演练活动,同时通过运维质量回访,及时调整运维策略。

B.2 场所条件

B.2.1 概述

条件许可的组织考虑建立独立的网络安全运维场所,以避免工作过程中安全保密信息违规扩散,提升网络安全工作人员协同效率。网络安全运维场所建设主要考虑两个方面:场所功能要求和场所安全要求。

B.2.2 场所功能

网络安全运维场所分为运维工作和指挥工作两类。

- a) 运维工作场所用于网络安全运维人员开展日常威胁事件监控、分析、调查等工作。运维场所在建设时考虑如下因素:
 - 1) 根据运维工作要求,宜为安全运维人员提供足够的操作空间,保证网络安全运维人员之间的沟通和协作;

- 2) 运维场所宜配备安全态势视屏墙,使用显示幕墙,集中化、可视化展现组织的网络安全态势和威胁感知信息,帮助安全运维人员及时了解安全动态,对风险进行预判;
 - 3) 根据监控分析的需求,运维场所宜为每名安全运维人员配置足够的操作终端,以显示监控仪表信息,操控各种威胁分析工具;
 - 4) 运维场所宜为安全运维人员的操作台面和座椅考虑人体工学因素,避免监控分析人员长期工作造成不良健康影响。
- b) 指挥工作场所用于发生网络安全事件时,管理人员决策处置方案,指挥调度处置工作等。运维指挥工作场所考虑配备相应的网络安全态势显示、威胁信息显示大屏,指挥操作终端,以及多渠道(如电话、视频会议、电子邮件、即时通信)的通信工具。指挥场所的要求包括:
- 1) 网络安全运维场所宜按照 GB/T 9361 和 GB/T 22239 中关于物理环境安全的要求进行建设;
 - 2) 网络安全运维场所设置访问控制机制配置人员访问权限;
 - 3) 网络安全运维场所配备门禁控制设备,限制和记录对网络安全运维场所的所有出入,并具备可调阅、查看实现回溯出入记录的能力;
 - 4) 在条件允许的情况下,可在网络安全运维场所的出入口安装防尾随设施;
 - 5) 网络安全运维场所安装闭路电视摄像头,监测和记录网络安全运维场所日常情况,并具备调阅、查看实现回溯视频记录的能力;
 - 6) 安全运维场所安装隔音材料,以避免内部通话信息外泄。

B.3 平台与工具

B.3.1 概述

安全运维的平台与工具是指为达到网络安全运维目标采用的系统或工具,主要功能包括传统信息安全管理、防护和运维等板块。在网络安全运维活动过程的整个过程中,可使用某种类型开源和商业化的平台、系统和工具,技术体系涉及的平台、系统和工具涵盖识别、防护、监测和响应领域的技术支撑。

B.3.2 资产管理类平台

对资产管理类平台的条件包括:

- a) 能够识别网络流量及探测、探针类设备上报的资产信息,实现多来源资产信息标准化输出;
- b) 能够根据资产部署位置、受攻击情况、防护情况等维度进行资产自动分级分类,发现重要、核心资产;
- c) 应用漏洞扫描工具和安全配置管理工具自动发现网络中的漏洞和安全配置问题。

B.3.3 态势感知类平台

对态势感知类平台的条件包括:

- a) 实现对流量数据、各类日志等对海量多源安全数据集中采集和存储,能够对安全数据进行查询、统计、关联分析,支持分析自定义分析规则;
- b) 能够通过威胁信息、机器学习、关联分析和基线分析等多个维度进行威胁的检测,提升威胁检测准确度,快速定位真正的威胁;
- c) 能够通过场景分析、实体分析、事件调查等威胁分析工具,结合安全运维工作实际场景,帮助提升安全事件研判和溯源的效率,及时进行响应处置;
- d) 能够帮助建立资产风险评估能力,实现资产安全风险综合评估,反映资产安全状态,以量化的

方式体现资产安全风险和安全工作成果；

- e) 能够帮助用户持续监测网络安全态势,为安全管理者提供风险评估和应急响应的决策支撑,为安全运维人员提供威胁发现、调查分析及响应处置的能力。部署网络安全防御平台或系统,包括加密与身份认证、防火墙、入侵检测和防御、DDoS 防御、Web 应用防火墙、防病毒系统、终端防护、漏洞扫描和修复等,以防止恶意攻击对网络 and 应用程序造成破坏等风险。

B.3.4 威胁检测类平台

对威胁检测类平台的条件包括：

- a) 支持全流量检测,对失陷主机、网络入侵、网络病毒、异常流量、异常行为等进行精准检测,及时识别出潜在的安全威胁；
- b) 支持基于攻击事件特征库和多维度事件分析技术,实时检测各种网络入侵及违规行为,可通过邮件、Syslog 等多种响应方式及时告警,实时、全面检测网络攻击,支持特征库升级；
- c) 能够提供基于 ATT&CK 标签分析告警的能力,并支持与其他系统联动,快速研判和处置告警事件；
- d) 能够发现、研判和处置重大安全事件,特别是针对新型网络攻击和 APT 攻击。应用大模型日志分析技术,通过预训练的大模型学习各种攻击和异常访问流程具备智能分析海量日志的能力,能够替代传统运维人员完成数据分析工作。

B.3.5 自动化处置工具

对自动化处置工具的条件包括：

- a) 将分散的工具、人员和流程有机地整合到一起,整合安全运维所需的各种资源,实现人与工具、工具与工具的连接与协作；
- b) 能够将安全操作流程或其片段转变成编排化的安全剧本,并尽可能自动化地执行,大幅降低安全运维人员的工作负担,提升工作效率；
- c) 能够便捷地对告警信息进行调查与增强,根据实战情况动态调整和组合剧本,更快速地进行告警分诊,提升单位时间内处理告警的数量和质量；
- d) 能够通过编排与自动化快速进行响应处置,实现安全运维效果的自动化、数字化度量,降低平均响应时长,提升运维水平；
- e) 能够自动记录所有对抗过程的操作记录,便于事后总结归纳,将有经验的安全运维人员的知识进行固化、沉淀、分享,并不断优化。

B.3.6 运维工具管理条件

对运维工具的管理条件包括：

- a) 建立运维工具的检测机制和能力,检测手段包括代码审查、恶意代码检测、沙箱分析等；
- b) 所有运维工具均需经过安全检测,通过后需登记备案,形成运维工具清单和运维工具库；
- c) 优先使用运维工具库中的工具,使用未登记备案的运维工具前先进行安全检测；
- d) 关键信息基础设施运维采用的工具符合 GB/T 39204—2022 中 7.9 的要求。

参 考 文 献

[1] GB/T 9361 计算机场地安全要求

[2] GB/T 20261—2020 信息安全技术 系统安全工程 能力成熟度模型

[3] GB/T 30283—2022 信息安全技术 信息安全服务 分类与代码

[4] GB/T 31495.2 信息安全技术 信息安全保障指标体系及评价方法 第2部分:指标体系

[5] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

[6] GB/T 42461—2023 信息安全技术 网络安全服务成本度量指南

[7] ITU-T X.1060 (06/2021) Framework for the creation and operation of a cyber defence centre



