ICS
CCS

T/SNISA

深圳市网络与信息安全行业协会团体标准

T/SNISA 04003—2025

电力行业外部攻击面运营管理指南

Guidelines for external attack surface management in electric power industry

草案版次选择

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

深圳市网络与信息安全行业协会　　发 布

目　　次

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。

本文件由深圳市网络与信息安全行业协会提出并归口。

本文件起草单位：深圳市润电信息科技有限公司、绿盟科技集团股份有限公司、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、中能融合智慧科技有限公司、深圳市魔方安全科技有限公司

本文件主要起草人：马雷博、邵科伟、廖志华、孙锐、黄国忠、陈达鑫、王磊、张春雷、崔康、沙雪松、鲍树楠、丁兴军。

引　言

国家战略和法规要求不断升级，电力等关键信息基础设施安全已上升至国家安全战略高度，电网瘫痪将引发医院停运、供水中断乃至社会动荡等连锁反应。《中华人民共和国网络安全法》《电力监控系统安全防护规定》《中华人民共和国关键信息基础设施安全保护条例》等法规对防护提出更高要求，构建新型防护体系已成国家安全战略亟需。

“云大物移智”正在重塑现在数字基础架构，网络边界越来越模糊。现有的安全防护体系存在不足，无法应对日益复杂的电力行业暴露面安全治理需求。同时，在开展外部攻击面运营管理方面普遍缺少规范性指导文件，部分机构在外部攻击面运营存在管理不到位的情况，并导致信息安全事件发生。因此有必要订制一个标准来指导行业提升外部攻击面运营管理能力，规范行业的外部攻击面运营管理工作。

综上，此标准的目的是建立一个可供电力行业各单位机构参考的外部攻击面运营管理指南，解决各单位机构在进行了一定程度安全建设后必须面临的外部攻击面深化治理带来安全挑战及痛难点问题，让行业的外部攻击面运营管理能力和水平在一定程度上螺旋上升。

电力行业外部攻击面运营管理指南

1 范围

本文件提供了电力行业开展外部攻击面运营管理中的互联网信息资产管理、攻击面识别与分析、攻击面收敛三个阶段涉及到的技术与管理手段的建设指导思路及方法。

本文件适用于电力行业的发电企业、输电企业、配电企业、售电企业、电力调度机构、电力交易机构等在完成基础的网络安全建设后开展的外部攻击面运营管理工作。

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 25069-2022 《信息安全技术术语》
- GB/T 36572-2018 《电力监控系统网络安全防护导则》
- GB/T 37138-2018 《电力信息系统安全等级保护实施指南》
- GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》
- GB/T 20984-2022《信息安全技术 信息安全风险评估方法》
- DL/T 2614-2023《电力行业网络安全等级保护基本要求》
- DL/T 2613-2023《电力行业网络安全等级保护测评指南》
- DL/T 2613-2023《电力行业网络安全等级保护测评指南》

3 术语和定义

GB/T 25069-2022中界定的以及下列术语和定义适用于本文件。

3.1

信息资产 information assets

客观存在于网络中，能被攻击者发现/利用，从而实现其系统破坏或非法获利目标的客体。

3.2

安全基线 security baseline

保障系统基本安全的最低配置要求。

3.3

攻击面 attack surface

所有可被攻击者利用来获取未经授权访问或实施攻击的漏洞、途径和方法的总和，包含技术、物理和人为因素。

3.4 **外部攻击面 external attack surface**

暴露于互联网，可被外部攻击者直接访问的资产和漏洞，如公网 Web 应用、开放端口、云存储错误配置。

3.5

网络安全漏洞 cybersecurity vulnerability

网络产品和服务在需求分析、设计、实现、配置、测试、运行、维护等过程中，无意或有意产生的、有可能被利用的缺陷或薄弱点。

3.6 **敏感信息 Sensitive Information**

一旦泄露、非法使用或篡改，可能导致个人权益受损、企业经济损失、公共利益受影响或国家安全风险的信息统称。

3.7 高危端口 High-Risk Port

易被攻击利用的网络端口，多因默认开放、服务漏洞或弱认证。

3.8 弱口令 Weak Password

易被猜测或工具破解的密码，缺乏足够复杂度与安全性。

3.9 风险优先级 Risk Priority

对已识别的安全风险，根据其潜在危害程度、发生可能性及管理成本，确定处置顺序的过程，核心目标是优先解决 “高影响、高概率” 风险。

3.10 攻击面识别 Attack Surface Identification

采用主动扫描、被动探测或资产梳理等方式，发现并确认系统、网络、资产中所有潜在攻击入口（漏洞、暴露端口、弱配置等）的过程，是攻击面管理的第一步。

3.11 攻击面收敛 Attack Surface Reduction

以风险为导向，通过识别、评估、处置和持续监控，减少组织可被攻击的入口与弱点，降低整体安全风险。

3.12 数字证书 Digital Certificate

由证书颁发机构(CA)签发的电子文件，包含实体身份信息、公钥、CA 签名及有效期，用于证明 “公钥归属” 及实体身份合法性。

4 缩略语

下列缩略语适用于本文件。

API: 应用程序接口（Application Programing Interface）

POC: 验证性测试（Proof of Concept）

URL: 统一资源定位系统（Uniform Resource Locator）

DMZ: 非军事化区（Demilitarized Zone）

APP: 应用程序（Application）

CNNVD: 中国国家信息安全漏洞库（China National Vulnerability Database of Infomastion Security）

CNVD: 国家信息安全漏洞共享平台（China National Vulnerability Database）

CVE: 通用漏洞披露（Common Vulnerabilities and Exposures）

CPE: 通用平台枚举（Common Platform Enumeration）

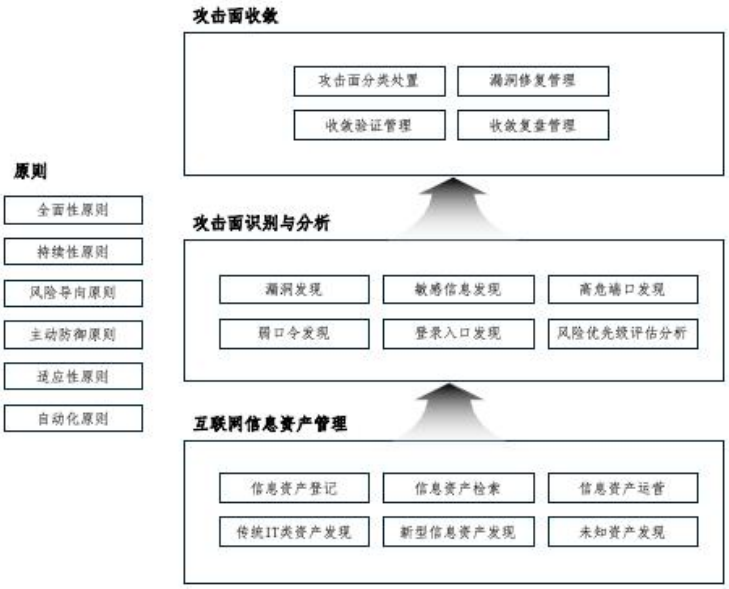
CVSS: 通用漏洞评分系统（Common Vulnerability Scoring System）

SDK: 软件开发工具包（Software Development Kit）

JAR: Java归档（Java Archive）

5 外部攻击面运营总体架构

本标准围绕电力行业关键基础设施高可靠、强合规的安全需求，构建“以暴露面可控为核心、以持续运营为手段、以风险收敛为目标”的外部攻击面运营管理体系。旨在通过科学的互联网资产梳理、以风险为导向的外部攻击面识别与分析、系统性的外部攻击面收敛工作，使外部攻击面运营管理体系化、规范化。在日常的安全工作中实践、检验、优化完善，提升组织的外部攻击面管理水平，确保组织的信息资产得到安全保护，为总体安全目标赋能。



体系以“互联网信息资产管理”为根基，全面厘清暴露于公网的IT资产与新型信息资产，确保“底数清、责任明”；以“攻击面识别与分析”为标尺，通过漏洞、弱口令、敏感信息、管理后台暴露等维度量化风险，实现“定位准、决策优”；以“攻击面收敛”为目标，采取下架、加固、访问控制、虚拟补丁等手动系统性缩小暴露面，达成“风险降、暴露少”。三者构成闭环运营链条，形成螺旋上升的持续改进机制，确保攻击面始终处于可知、可管、可控状态。

架构聚焦提升电力企业对外部威胁的预见性、响应效率与资源投入精准度，降低因暴露面失控导致的重大安全事件概率，为构建“实战化、体系化、常态化”的新型电力安全防护体系提供核心支撑，助力行业实现安全与发展的动态平衡。

6 外部攻击面运营管理原则

6.1 全面性原则

应覆盖所有攻击面类型，包括传统IT类资产和新型信息资产（如移动端APP、微信小程序等）。

6.2 持续性原则

外部攻击面运营管理是一个持续的过程，而不是一次性的活动。应通过持续性的检测和监测，以应对复杂、动态的外部攻击面。

6.3 风险导向原则

外部攻击面运营应以风险管理为核心，识别发现、评估控制网络安全风险。应将有限的资产集中到高风险的攻击面上。

6.4 主动防御原则

攻击面管理应强调主动发现和防御，例如通过模拟攻击、漏洞验证、情报驱动等手段来识别和降低风险。

6.5 适应性原则

应根据企业的具体情况进行调整和优化，例如机构的规模、行业、安全需求等进行综合评估。

6.6 自动化原则

宜尽可能地自动化地应用攻击面工具及技术手段，例如自动化资产发现、自动化漏洞识别、自动化风险评估等，以提升运营效率。

7 互联网信息资产管理

7.1 互联网信息资产识别目标

发现、识别、梳理互联网暴露面的信息资产，形成完备的信息资产数据库。周期性地执行信息资产盘点任务，覆盖传统的 IT 资产，如：公网 IP、子域名等，也应覆盖新型的信息资产，如：公众号、小程序、APP 等。最后，通过资产线索扩展资产巡查以发现未知资产，从而提升组织对互联网信息资产的安全运营管理能力。

7.2 互联网信息资产管理过程

7.2.1 传统 IT 类资产发现

互联网传统IT类资产发现的目的，是对组织互联网暴露面进行全面掌握，以更好地开展安全风险识别和处置工作。互联网信息资产发现方式，包括：

a) 主动发现：应通过网络空间测绘技术，发现互联网及内网 DMZ 区中的 IP、开放端口、协议、证书、子域名、URL、中间件及 Web 框架等信息；
b) 被动发现：宜通过流量监听的方式被动发现网络中的信息资产；
c) 人工梳理：应通过人工的方式，对互联网信息资产进行收集、梳理。

7.2.2 新型信息资产发现

互联网新型信息资产发现的目的，是进一步加深对互联网暴露面的掌握，以更好地开展安全风险识别和处置工作。

a) 新应用发现：应通过机构名称、LOGO、开发者等资产线索，通过自动化工具，对移动端 APP、小程序自动化检索，并进行筛选收录，纳入正常的安全管理范畴。同时，宜在内部发起人工上报流程，对目前机构内部进行收集备案；
b) 新媒体发现：应通过机构名称、LOGO、开发者等资产线索，通过自动化工具，对微信公众号、微博账号等社交媒体资产进行自动化检索，并进行筛选收录，纳入正常的安全管理范畴。同时，宜与宣发部门沟通，获取所有的媒体矩阵账号，形成更完善的媒体资产台账。

7.2.3 未知资产发现

随着数字化转型的深入，电力系统可控对象从以源为主扩展到源网荷储各环节，控制规模呈指数级增长，调控技术手段和配套的数字设施数量日益增加、种类丰富、变动频繁，应重点关注以下重点场景：

a) 私搭乱建排查：应通过机构名称、LOGO、证书签名等资产线索，采用自动化工具/人工检索在网络空间中重点筛查含有机构特征的网站或接口；
b) 老旧、闲置、退役资产排查：宜尽可能下线闲置、老旧资产，与业务部门沟通，对可下线的信息系统关停。应对退役资产、已下线流程中的资产进行网络存活探测，防止资产因误操作再度上线。应通过退役资产名称、LOGO、证书签名等资产线索，采用自动化工具/人工检索在网络空间中重点筛查含有机构特征的网站或接口；
c) 测试系统、演示系统排查：宜对开发测试环境的系统进行清点，通过系统名称、LOGO、证书签名等资产线索，通过自动化工具/人工检索在网络空间中重点筛查含有机构特征的网站或接口，进行重点筛查，避免此类系统被映射到互联网中。

7.2.4 互联网信息资产登记

应对互联网信息资产进行业务及负责人登记，有助于提升应急响应效率。互联网信息资产登记包括以下维度：

a) 业务关系登记：应对互联网信息资产所承载的业务系统进行登记。若业务呈复杂的树状结构，宜整理其完整的依赖关系，并详细登记；

b) 业务负责人登记：应对互联网信息资产负责人进行登记。登记角色应包括：业务系统开发负责人、业务系统运维负责人、业务系统网络运维负责人，及其联系方式。

7.2.5 互联网信息资产检索

应建立对互联网信息资产快速检索能力,检索有助于快速定位存在风险的资产,并加快后续的处置效率。互联网信息资产检索包括以下维度检索条件：

a) 基础数据维度：子域名、主域名、IP、开放端口、URL、服务、协议等；
b) 管理维度：应用系统名称、系统负责人、互联网开放情况等；
c) 风险维度：是否存在安全漏洞等。

7.2.6 互联网信息资产运营

互联网信息资产运营宜遵循以下：

a) 数字证书管理：宜对数字证书的申请、发放、使用、注销等做统一管理，保障数字证书的可用性、完整性、保密性；
b) 信息资产变动监测：应对互联网信息资产的变动进行持续监测，对比上一轮次的监测结果进行比对，标记出“新增”、“减少”及“不变”等的变动状态。方便针对新上线资产、退网资产进行跟踪管理；
c) 重点资产监测：应标记重点资产，设置更高频率的监测任务，进行重点管理；
d) 设置告警：宜根据管理要求，设置告警条件阈值，在出现超过告警阈值的事件时，发送告警信息，便于及时发现互联网信息资产的异动情况。

7.3 互联网信息资产管理优良实践

互联网信息资产的优良实践，包括以下：

a) 互联网信息资产管理是外部攻击面的主要基础工作之一，宜持续对信息资产进行跟踪和维护；
b) 宜使用成熟的基于生命周期的方法，对信息资产进行管理，确保信息资产为最新状态；
c) 在互联网资产管理过程中，宜采用自动化收集的方法/工具，提升管理效率；
d) 可采用集中管理系统进行统一管理，采用 API 调用方式从其他信息系统及时获取最新信息；
e) 宜与内部 IT 运营流程进行联动，使得互联网信息资产输入、变更等能得到及时的更新，从而确保信息的准确。

8 攻击面识别与分析

8.1 攻击面识别与分析目标

攻击面识别是所有互联网信息资产进行所有可能被攻击者的攻击面向量进行识别，例如漏洞、配置缺陷、弱口令、身份和访问管理缺陷等。攻击面识别是攻击面管理的重要环节，尽可能识别出所有的攻击向量，才能更有效地进行风险评估和安全防护。

8.2 攻击面识别与分析管理过程

8.2.1 漏洞发现

漏洞发现是攻击面识别的重要环节，应通过以下方式及时发现系统中存在的漏洞，避免系统漏洞长期暴露。漏洞发现方式包括但不限于：

a) POC 漏洞检查：应利用漏洞情报或自动化工具配套的 POC 检测插件，对可疑信息资产组进行针对性地扫描，快速定位风险信息资产；
b) 基于漏洞库的版本比对检查：应与 CNNVD、CNVD 或 CVE 等漏洞库通过 CPE 对资产数据进行全量匹配，获得受影响的资产漏洞列表。

8.2.2 敏感信息泄露发现

敏感信息泄露发现是攻击面识别中容易被忽略的环节，可能存在配置文件、内部机密文件等重要信息被泄露，为有效识别和发现此类敏感信息泄露情况，应重点关注以下三个方面的检索工作：

a) 代码仓库检索：宜通过收集内部通用的 SDK、特定的 JAR 包与类名、电力调度相关作业系统名称等方式制定具有本机构特色的代码资产线索，采用自动化工具/人工检索在常用的开源社区平台，进行重点筛查；
b) 文库检索：宜通过收集内部文档命名规则、机构名称、文档编号等方式制定资产线索，采用自动化工具/人工检索在常用的文档文库共享平台，进行重点筛查含有机构特征的疑似文档；
c) 网盘检索：宜通过机构名称、电力调度相关作业系统名称等方式资产线索，采用自动化工具/人工检索在常用的网盘资源享平台中，进行重点筛查含有机构特征的疑似项目。

8.2.3 高危端口发现

高危端口发现是识别互联网暴露面中可能被攻击者利用的关键入口点，应重点关注可能存在安全风险的开放端口及其对应服务。高危端口发现方式包括但不限于：

a) 常见高危端口扫描：应重点检测互联网暴露的高危端口的开放情况；
b) 电力行业特有端口检测：宜重点关注电力行业特有系统等相关的专用端口的暴露情况；
c) 非标准端口服务识别：应对非标准端口上运行的服务进行指纹识别，发现可能存在的数据库、Web 服务、远程管理等高风险服务；

8.2.4 弱口令发现

弱口令发现是攻击面识别中的关键环节，弱口令是攻击者获取系统访问权限的常见入口，应重点识别互联网信息资产中存在的弱口令、默认口令等身份认证安全风险。弱口令发现方式包括但不限于：

a) 常见弱口令检测：应针对 Web 登录界面、数据库、FTP、SSH、RDP 等服务进行常见弱口令检测；
b) 默认口令检测：宜重点检测设备厂商的默认口令，包括网络设备、安全设备、服务器、数据库等的出厂默认凭证；
c) 电力行业特定弱口令检测：应关注电力行业专用系统的常见弱口令；
d) 基于机构信息的口令检测：宜结合机构名称、电话号码、地址信息等构建针对性字典，检测可能使用机构相关信息作为口令的情况；

8.2.5 登录入口及管理后台发现

管理后台发现是攻击面识别中的重要环节，管理后台通常具有较高的系统权限，一旦被攻击者发现并获得访问权限，可能造成严重的安全事件。应重点识别互联网暴露的各类管理后台及控制界面。管理后台发现方式包括但不限于：

a) 常见管理后台路径检测：应检测常见的管理后台访问路径，如：/admin、/manager、/console、/management、/backend、/cp、/wp-admin 等；
b) 设备管理界面发现：宜重点检测网络设备、安全设备、服务器等的 Web 管理界面，如路由器、交换机、防火墙、UPS、摄像头等设备的管理后台；
c) 应用系统管理界面发现：应识别各类应用系统的管理后台，包括数据库管理工具（如 phpMyAdmin、Adminer）、中间件管理控制台（如 Tomcat Manager、WebLogic Console）等；
d) 电力专用系统管理界面发现：宜重点关注电力调度系统、SCADA 系统、能源管理系统、配电自动化系统等专用系统的 Web 管理界面。

8.2.6 风险优先级评估分析

风险优先级评估是对发现的攻击面进行风险等级划分，确保有限的安全资源优先处置高风险攻击面。风险优先级评估应综合考虑以下因素：

a) 资产重要性评估：宜根据资产承载的业务重要性进行分级，重点关注电力调度、电网监控等核心业务系统；
b) 漏洞攻防价值评估：POC 检测插件发现的漏洞一般为可复现且攻防价值较高的漏洞，宜优响应处置；其他漏洞结果数据集，参考 CVSS 评分模型、DREAD 模型等进行综合评估；
c) 威胁活跃度评估：宜结合漏洞情报进行评估，优先处置攻击者高度关注或正在被恶意利用的风险；
d) 修复难易程度评估：宜综合考虑攻击面修复的业务影响程度和技术难度，优先处置风险大、易修复的攻击面。修复难易程度评估包括：技术复杂度（是否需要系统停机、是否涉及核心

代码修改、是否需要第三方厂商支持等）；业务连续性影响（修复过程是否影响电力生产运行、是否需要业务中断、修复窗口时间要求等）进行综合评估。

8.3 攻击面识别与分析优良实践

攻击面识别与分析的优良实践，包括以下：

a) 情报适配：宜利用漏洞情报中的资产影响范围，自动化匹配疑似的互联网信息资产。对于需要进行 POC 验证的漏洞，可以通过圈定高疑似的资产数据范围，有效缩减 POC 检测的信息资产范围与数量，提升 POC 漏洞的检测效率；

b) 优先识别具有利用细节的漏洞：宜优先识别可复现、可利用的漏洞结果，在漏洞确认环节尽可能获取细节信息，如：URL 地址、详细报文等，方便复现与后续的修复验证工作；

c) 整理软件供应链数据库：宜对调度系统、企业应用系统、营销系统等进行供应商及版本持续的识别，当出现漏洞情报时，将加快应急响应效率。

9 攻击面收敛

9.1 攻击面收敛目标

攻击面收敛的目标是通过技术手段和管理措施，主动减少互联网暴露的攻击面，降低被攻击者利用的风险。通过系统性的攻击面收敛工作，最小化机构对外暴露的攻击向量，提升整体安全防护水平。攻击面收敛应实现以下目标：最小化暴露原则，仅保留业务必需的互联网暴露面；及时消除安全风险，对发现的高风险攻击面进行快速处置；建立纵深防御体系，形成多层次的安全防护机制；提升安全运营效率，通过攻击面收敛减少日常安全运营工作量。

9.2 攻击面收敛管理过程

9.2.1 攻击面分类处置

应根据攻击面的风险等级和处置方式进行分类管理，制定差异化的处置策略。攻击面分类处置包括：

a) 业务下线类：对于存在严重安全风险且无业务价值的系统，如应下线但未下线、长期无人运营、演示环境、测试环境等系统，应立即下线处理；

b) 投诉下架类：对于在第三方平台发现的敏感信息泄露，应通过官方渠道进行申诉下架处理。包括在开源代码仓库发现的源代码泄露、在文档分享平台发现的内部文档泄露、在网盘资源平台发现的项目文件泄露等情况，应及时联系平台客服或通过官方举报渠道申请删除相关泄露内容；

c) 加固修复类：对于具有业务价值但存在安全风险的攻击面，应通过技术加固、补丁修复等方式消除风险，如系统漏洞修复、弱口令整改、权限控制加强等；

d) 访问控制类：对于必须保留但风险较高的攻击面，应通过访问控制手段限制暴露范围，如 IP 白名单、VPN 访问、双因素认证等；

9.2.2 漏洞修复管理

漏洞修复是攻击面收敛的核心环节，应建立完善的漏洞修复管理流程。漏洞修复管理包括：

a) 根据风险优先级进行工单派发：宜针对严重高危漏洞制定修复方案，包括修复方式、修复时间、回退方案等内容，附于工单进行流转；

b) 组件升级修复：应通过将漏洞载体升级到最新版本，以消除漏洞。

c) 虚拟补丁修复：应通过前置防护设备有效控制用户与漏洞载体的输入输出，阻断可能存在的漏洞利用情况；

d) 策略阻断：应通过网络防护策略对漏洞载体的访问权限进行控制，根据业务需求限制允许访问漏洞载体和允许漏洞载体访问的地址范围；

e) 升级补丁修复：应通过官方渠道获取漏洞修复补丁，以对漏洞载体进行补丁升级的方式修复漏洞；

f) 配置整改修复：通过加固引发风险的配置项，以消除风险。

9.2.3 收敛验证管理

收敛验证是验证风险修复工作的有效性，避免因为执行操作、修复加固失败、系统重新部署等情况导致漏洞复发，形成安全管理盲区。收敛验证工作包括但不限于：

a) 利用自动化能力以漏洞扫描的方式进行复测；
b) 以人工验证的方式进行复测；

9.2.4 收敛复盘管理

攻击面收敛复盘是总结风险发现、验证、加固和复测每个过程的操作，识别可以改进的环境，持续优化攻击面收敛运营工作：

收敛验证是验证风险修复工作的有效性，避免因为执行操作、修复加固失败、系统重新部署等情况导致漏洞复发，形成安全管理盲区。收敛验证工作包括但不限于：

a) 根据风险发现的过程、风险产生的原因、控制措施的有效性几个方面进行复盘；
b) 针对在复盘的过程中发现的问题，进行迭代优化和整改。

9.3 攻击面收敛优良实践

攻击面收敛的优良实践，包括以下：

a) 建立持续收敛机制：攻击面收敛应建立持续性工作机制，定期开展攻击面评估和收敛工作，确保攻击面始终保持在可控范围内；
b) 加强部门协作配合：攻击面收敛工作涉及多个部门，应建立有效的协作机制，确保各部门职责明确、配合密切；
c) 自动化漏洞复测：宜通过自动化工具对研发/测试反馈进行初步修复/加固工作后，自助调用检测引擎进行漏洞复测；

参 考 文 献

[1] GB/T 36572-2018，电力监控系统网络安全防护导则〔S〕
[2] GB/T 38318-2019，电力监控系统网络安全评估指南〔S〕
[3] GB/T 39204-2022，信息安全技术 关键信息基础设施安全保护要求〔S〕
[4] GB/T 22239-2019，信息安全技术 网络安全等级保护基本要求〔S〕
[5] DL/T 2613—2023，电力行业网络安全等级保护测评指南〔S〕
[6] DL/T 2614—2023，电力行业网络安全等级保护基本要求〔S〕
[7] Against Data Attacks on Smart Grid Operations: Attack Mechanisms and Security Measures〔M〕.SpringerLink, 2023:1-15
[8] International Standards for Cybersecurity in Smart Devices for the Power Sector〔C〕//2024 International Conference on Computational Intelligence for Green and Sustainable Technologies (ICCIGST).IEEE Xplore, 2024
[9] Protecting Energy Infrastructure: CESER, Partners Publish Cybersecurity Guidance to Mitigate Cyber-Attacks〔R〕.U.S. Department of Energy, 2025-01-17
[10] 电力系统供应链攻击防范：APT 攻击的新途径与防御策略〔J〕.CSDN 文库，2025 (3):1-8