ICS 35.030
CCS L80

DB3309

浙 江 省 舟 山 市 地 方 标 准

DB 3309/T 110—2024

网络攻击诱捕系统管理规范

2024－11－5 发布　　2024－12－5 实施

舟山市市场监督管理局　　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。

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。

本文件由舟山市公安局提出并归口。

本文件起草单位：舟山市公安局，北京元支点信息安全技术有限公司。

本文件主要起草人：张艳波，王翘楚，张通汉，何淼楹，施翔，丁峰，杨丁源，杨柯，任俊博，林建伟，史晨伟，黄林。

网络攻击诱捕系统管理规范

1 范围

本文件规定了网络攻击诱捕系统的人员要求、设施和设备要求、管理流程和系统运维。

本文件适用于网络攻击诱捕系统的运行和管理。

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/Z 23283 基于文件的电子信息的长期保存

GB/T 25068.2 信息技术 安全技术 网络安全第2部分：网络安全设计和实现指南

GB/T 25069—2022 信息安全技术 术语

GB/T 26163.1 信息与文献 文件管理过程 文件元数据 第1部分：原则

GA/T 756 法庭科学 电子数据收集提取技术规范

GA/T 1170 移动终端取证检验方法

GA/T 1174 电子证据数据现场获取通用方法

DB 3309/T 109—2024 网络攻击诱捕系统建设规范

3 术语和定义

GB/T 25069—2022和DB 3309/T 109—2024界定的以及下列术语和定义适用于本文件。

3.1

网络攻击诱捕系统

一种网络安全技术，旨在通过创建虚假资源来吸引和误导潜在攻击者，从而检测、延迟和分析攻击行为。

4 人员要求

4.1 岗位要求

4.1.1 应设立系统管理负责人，对整个网络攻击诱捕系统负全责。

4.1.2 应设立系统管理员、安全运营管理员、安全审计员等岗位，并设置各个工作岗位的职责。

4.1.3 应制定管理文件明确各岗位的任职资格和技能要求。

4.2 工作内容

4.2.1 应配备系统管理员，负责的工作内容包括：

a) 系统参数维护和管理；

b) 用户的注册、删除，组织机构的变动调整；

c) 与用户权限相关的各类角色的设置。

4.2.2 应配备安全运营管理员，负责的工作内容包括：

a) 安全运营管理；
b) 安全告警事件管理和处置；
c) 威胁检测、预警、决策、处置流程的闭环管理。

4.2.3 应配备安全审计员，负责的工作内容包括：

a) 审核系统管理员、安全运营管理员的操作审批单；
b) 监督检查系统管理员、安全运营管理员等的操作过程和操作日志；
c) 处理系统自动产生的非法操作报警；
d) 审核系统日志，每周至少 1 次；
e) 定期备份系统日志，每个月不少于 1 次；
f) 提出系统非法操作报警的参数修改建议。

4.3 人员管理

4.3.1 上岗人员应具备计算机网络、信息安全专业知识。

4.3.2 上岗前应对人员进行背景审查和安全行为规范培训，形成培训记录并归档管理。

4.3.3 应定期对上岗人员进行考核，并对考核结果进行记录并保存。

4.3.4 上岗人员离岗应进行安全审计并归档管理。

5 设施和设备要求

5.1 管理要求

应制定设施设备注册、配置、统计、状态查询、测试、诊断等制度，并定期对设施设备进行维护。

5.2 设施设备

5.2.1 网络攻击诱捕系统配套设施设备包括但不限于虚拟机、服务器等。进行网络终端部署时，所支持的设备包括但不限于台式计算机、摄像头、执法记录仪等。

5.2.2 服务器设备应至少满足以下要求：

a) 中央处理器：16 个及以上核心数；
b) 内存：64 GB 及以上；
c) 硬盘：8 TB 及以上；
d) 网络：2 个及以上千兆网卡；
e) 电源：双电源。

6 管理流程

6.1 网络安全设计

网络攻击诱捕系统整体设计应符合GB/T 25068.2的要求。

6.2 终端威胁感知

应明确网络攻击诱捕系统的威胁感知需求，从而符合DB3309/T 109-2024终端威胁感知的要求。

6.3 蜜罐功能

应明确网络攻击诱捕系统的蜜罐功能需求，从而能够符合DB3309/T 109-2024蜜罐功能的要求。

6.4 数据分析

应能够对网络攻击诱捕系统获取的数据进行有效分析，从而能够为系统用户了解当前网络安全态势提供依据和支撑。

6.5 事件处置

6.5.1 处理机制

应制定网络安全事件处理预案，在网络攻击诱捕系统检测到网络安全事件后，能够进行有效处置，预案至少应包括取证、处理和上报。

6.5.2 取证

6.5.2.1 网络攻击诱捕系统的取证应符合 GA/T 756、GA/T 1170 和 GA/T 1174 的要求。

6.5.2.2 对发现的高危、攻陷类告警应及时上报，并协调网络安全应急力量进行处置，隔离受入侵设备，并对相关区域进行全面排查，消除隐患。

6.6 数据保存

网络攻击诱捕系统产生的数据应按GB/Z 23283和GB/T 26163.1的要求保存。

6.7 检查与演练

6.7.1 应定期按网络安全事件处理预案进行检查，以确保预案能够得到有效执行，检查周期每年不少于 4 次。

6.7.2 应定期演练网络安全处理预案，演练周期宜不少于每年 2 次。

6.8 数据呈现

应提供数据呈现机制，将安全态势、网络威胁等情况，通过数据可视化方式，为相关部门领导决策指挥提供数据支持。

7 系统运维

7.1 应制定系统维护、升级和检查的方案。

7.2 每周应进行至少一次系统的巡检，检查服务器的运行状态、系统运行状态，并填写巡检记录表。巡检记录表示例参见附录 A。

7.3 应至少每月一次对系统进行全面检查，检查内容应包括功能、日志的情况等，填写检查记录表。检查记录表的示例参见附录 B。

7.4 系统升级前应确认系统升级类型、升级内容，在运维测试环境下验证升级方案的可行性。

7.5 升级完成后，应确认系统的可用性，制定升级后的试运行周期，开展持续监测。

参 考 文 献

[1]《中华人民共和国网络安全法》
[2]《中华人民共和国数据安全法》

附 录 A
（资料性）
巡检记录表

系统名称		巡检方式	
巡检日期		巡检人	
巡检时间			
巡检结论			
存在、遗留问题及解决方法			
负责人确认			

检查对象	检查项	检查结果	参考值
外观	外壳、机身		外壳：无损坏 机身：固定良好，螺丝、卡扣无松动
	设备运转		声音无明显异常
	硬盘指示灯		闪烁
	电源指示灯		绿灯常亮
	网卡指示灯		双灯：一灯常亮、一灯闪烁 单灯：闪烁
配置及资源	系统 IP 地址		按规定分配，无冲突
	软件版本		与更新记录一致
	固件版本		与更新记录一致
	口令		使用强口令
	运行记录		根据设备实际情况填写
	许可状态		许可没有过期
	资源信息		CPU、内存占用一般应小于 90% 磁盘 IO 负载一般应小于 70%
	存储空间		存储空间>50G

附 录 B
（资料性）
检查记录表

系统名称		检查方式	
检查日期		检查人	
检查时间			
检查结论			
存在、遗留问题及解决方法			
负责人确认			

检查对象	检查项	检查内容	检查结果
登录与使用	登录情况	WEB 页面登录是否正常	
	使用状态	检查运行状态、蜜罐运行状态、牵引器运行是否启动	
日志相关	告警日志	告警日志产生是否正常	
	审计日志	审计员登录查询审计日志是否正常记录操作日志	
	磁盘使用率	系统滚动清理是否正常	
	上报	上报日志生成是滞正常	
流量牵引器	流量牵引器连接状态	查看流量牵引器下设备连接状态是否为已连接	
	下级连接状态	查看下级设备是否为已连接状态	
服务	控制台	各服务状态是否正常显示	
	蜜罐	查看蜜罐状态是否为已连接状态	