



# 中华人民共和国公共安全行业标准

GA/T XXXX—XXXX  
代替 GA/T 911-2010

## 信息安全技术 日志分析产品安全技术要求

Information security technology Security technical requirements for log analysis  
products

(报批稿)

行业标准信息服务平台

XXXX - XX - XX 发布

XXXX - XX - XX 实施

中华人民共和国公安部 发布



## 目 次

前言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 总体说明 .....	2
4.1 安全技术要求分类 .....	2
4.2 安全等级划分 .....	2
5 安全功能要求 .....	2
5.1 日志采集和存储 .....	2
5.2 日志分析和处理 .....	4
5.3 日志呈现和报警 .....	5
5.4 开发接口 .....	6
6 自身安全功能要求 .....	6
6.1 组件安全 .....	6
6.2 安全管理 .....	6
6.3 自身审计功能 .....	7
6.4 系统报警 .....	8
7 安全保障要求 .....	8
7.1 开发 .....	8
7.2 指导性文档 .....	9
7.3 生命周期支持 .....	10
7.4 测试 .....	11
7.5 脆弱性评定 .....	11
8 等级划分要求 .....	12
8.1 概述 .....	12
8.2 安全功能要求等级划分 .....	12
8.3 自身安全功能要求等级划分 .....	13
8.4 安全保障要求等级划分 .....	13