Chinastandards.org

ICS 35.240
CCS A 90

GA

INDUSTRY STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GA/T 911-2010

Information security technology - Security technical requirements for log analysis products

信息安全技术 日志分析产品安全技术要求

(English Translation)

Issued on: January 1, 1970 **Implemented on: March 19, 2019**

Issued by: Ministry of Public Security

Preview: page 1 of 5 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-911-2010

Chinastandards.org

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 General description
4.1 Classification of safety technical requirements
4.2 Classification of Security Levels.
5 Safety function requirements
5.1 Log Collection and Storage
5.2 Log Analysis and Processing
5.3 Log presentation and alarm
5.4 Development Interface
6 Self-safe function requirements
6.1 Component safety
6.2 Security management
6.3 Self audit function
6.4 System alarm
7 Security requirements
7.1 Development
7.2 Guidance documents
7.3 Life cycle support
7.4 Testing
7.5 Vulnerability assessment
8 Classification requirements
8.1 Overview
8.2 Safety function requirements classification
8.3 Classification of self-safety function requirements
8.4 Classification of security requirements

Preview: page 2 of 5 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-911-2010

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard replaces GA/T 911-2010 "Information security technology log analysis product security technical requirements", compared with GA/T 911-2010 the main changes are as follows.

-Revised the requirements of "level division" to divide the level into two levels. basic level and enhanced level (see Chapter 8, 2010 version 7.2, 7.3 and 7.4);

-Removed the requirement for "standard protocol reception" (see 4.1.2.1 of the 2010 version);

-Removed the requirement of "agent collection" (see 4.1.2.2 of the 2010 version);

-Removed the requirement for "log file import" (see 4.1.2.3 of the 2010 version);

-Added requirements for "data collection" (see 5.1.2.1);

-Revised the requirements for "backup of audit records" (see 5.1.6, 4.2.3 of the 2010 edition);

-Removed the "self-protection ability of software agents" requirement (see 5.1.1.1 of the 2010 version);

-Removed the "data transmission control" requirement (see 5.1.1.3 of the 2010 version);

-Removed the requirement for "data resumption" (see 5.1.1.4 in 2010);

-Added requirements for "multi-level deployment" (see 6.1.1);

-Added the requirement of "multiple authentication" (see 6.2.1.3);

-Added the requirement of "timeout lock" (see 6.2.1.4);

-Removed the requirement for "storage of audit records" (see 5.3.2 of the 2010 edition);

-Removed the "audit management" requirement (see 5.3.3 of the 2010 edition);

-Added the requirement of "data storage security" (see 6.3.3).

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security.

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

This standard was drafted. Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security, Hangzhou Anheng Information Technology Co., Ltd., Huawei Technologies Co., Ltd.

Preview: page 3 of 5 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-911-2010

1 Scope

This standard specifies the safety function requirements, self-safety function requirements, safety guarantee requirements, and classification requirements for log analysis products.

This standard applies to the design, development, and testing of log analysis products.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 18336.3-2015 Information technology security technology Information technology security assessment guidelines Part 3. Security assurance components GB/T 25069-2010 Information Security Technology Terminology

3 Terms and definitions

GB/T 18336.3-2015 and GB/T 25069-2010 and the following terms and definitions apply to this document.

Log analysis product Collect log data in the information system through log agents, standard protocols, file import, etc., and perform centralized storage and analysis.

Security products.

Log data source

The original source that produced the log data.

Log administration center A functional module for centralized processing, storage, and analysis of collected log data.

Audit log

Log analysis log data generated by the product's own audit.

Log record

After preprocessing the collected raw log data, log data is generated and stored in the log management center according to certain rules.

Authorized administrator A user with log analysis product management authority is responsible for managing the system configuration, security policy, and log data of the log analysis product Management.

Preview: page 4 of 5 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-911-2010

4.1 Classification of safety technical requirements

This standard divides the log analysis product security technical requirements into three categories. security functions, own security functions, and security assurance requirements. among them, Security function requirements are specific requirements for the security functions that log analysis products should have, including log collection and storage, log record processing, Log presentation, alarm and development interface, etc .; the self-security function is to put forward specific requirements for the self-security function that the log analysis product should have Including component security, management, self-auditing functions, and system alarms; security guarantees are required for log analysis products the process puts forward specific requirements, such as development, guidance documents, life cycle support, testing, and vulnerability assessment.

4.2 Classification of security levels

The security level of the log analysis product is divided into bases based on the strength of its security function requirements, its own security function requirements, and security assurance requirements.

This level and enhanced level, in which the security requirements refer to GB/T 18336.3-2015.

5.1.1 Log data source

Log analysis products should be able to add, modify, and delete management operations on the log data source, and the type of log data source should be at least Contains the following ranges.

a) network equipment, such as switches, routers, firewalls;

b) operating system;

c) database system;

d) other application systems.

5.1.2.1 Data collection

Log analysis products should be able to collect log data from log data sources in a certain way, including at least one of the following collection methods.

a) log agent;

b) standard agreements;

c) file import;

d) other.

Preview: page 5 of 5 shown, 13 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-911-2010