Chinastandards.org

ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

chinastandards.org - PREVIEW

GB/T 42453-2023

Information security technology - General technical requirements for network security situation awareness

信息安全技术 网络安全态势感知通用技术要求

Issued on: March 17, 2023 **Implemented on: October 1, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Preview: page 1 of 5 shown, 18 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-42453-2023

Table of Contents

chinastandards.org · PREVIEW

Foreword

This document was issued on 17 March 2023 by the State Administration for Market Regulation; Standardization Administration of the PRC and takes effect on 1 October 2023.

It is a GB/T standard: recommended rather than compulsory, but it is the text a Chinese reviewer applies when assessing a submission.

1 Scope

GB/T 42453-2023 covers the make-up of a network security situation awareness system, the platform that gathers what a defended network is reporting and turns it into a picture somebody can act on. A framework clause names the parts: the front-end data sources, the core components that do the work, and the other elements around them. The requirements then follow the path the data takes through those components - data aggregation, data analysis, situation display, monitoring and warning, the data service interfaces through which results are handed to other systems, and the management of the platform itself. Terms build on GB/T 25069-2022, with threat and the rest defined here, and the abbreviations used across the requirements are listed separately. The ordering reflects where awareness actually breaks down: data collected from sources that never agreed on a format and so cannot be correlated, analysis that produces alerts nobody has defined a

Preview: page 2 of 5 shown, 18 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-42453-2023

threshold for, or a display that shows everything at once and therefore shows nothing. Naming a requirement for each stage makes a platform assessable rather than merely demonstrable. For operators of critical information infrastructure, security platform vendors, system integrators, and the assessors who evaluate a deployment before it is trusted.

This document provides a technical framework for network security situation awareness and

stipulates the general technical requirements for core components in the framework.

This document is applicable to the planning, design, development, construction and assessment

of network security situation awareness products, systems or platforms.

chinastandards.org · PREVIEW

2 Normative References

The contents of the following documents constitute indispensable clauses of this document

through the normative references in this text. In terms of references with a specified date, only

versions with a specified date are applicable to this document. In terms of references without a

specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 25069-2022 Information Security Techniques - Terminology

GB/T 28458-2020 Information Security Technology - Cybersecurity Vulnerability

Identification and Description Specification

GB/T 28517-2012 Network Incident Object Description and Exchange Format

GB/T 30279-2020 Information Security Technology - Guidelines for Categorization and

Classification of Cybersecurity Vulnerability

GB/T 36643-2018 Information Security Technology - Cyber Security Threat Information

Format

GB/T 37027-2018 Information Security Technology - Specifications of Definition and

Description for Network Attack

3 Terms and Definitions

What is defined in GB/T 25069-2022, and the following terms and definitions are applicable

Preview: page 3 of 5 shown, 18 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-42453-2023

to

this document.

3.1 threat

Threat refers to a potential factor of undesired incident that may cause harm to a system or

organization.

[source: GB/T 25069-2022, 3.628]

3.2 threat information

Threat information is evidence-based knowledge used to describe existing or possible threats,

so as to achieve response and prevention of threats.

NOTE: threat information includes context, attack mechanism, attack indicator and possible impact,

etc.

[source: GB/T 36643-2018, 3.3, modified]

3.3 network security situation awareness

Network security situation awareness means analyzing and processing network behavior and

user behavior and other factors, grasping network security status and predicting network

security trends by collecting data, such as: network traffic, asset information, logs, vulnerability

information, warning information and threat information, etc., and carrying out activities of

displaying and monitoring warnings.

3.4 front-end data source

Front-end data source refers to software and hardware providing data to the core components

of network security situation awareness.

3.5 profiling

Profiling refers to a process of constructing descriptive labeling attributes of a certain type of

object in multiple dimensions, utilizing these labeling attributes to analyze the multi-faceted

chinastandards.org · PREVIEW

Preview: page 4 of 5 shown, 18 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-42453-2023

characteristics of the object, and abstracting and generalizing its full picture.

3.6 warning

Warning refers to alarms issued in advance or in a timely manner for upcoming or ongoing network security incidents or threats.

[source: GB/T 25069-2022, 3.739]

4 Abbreviations

The following abbreviations are applicable to this document.

CPU: Central Processing Unit

FTP: File Transfer Protocol

FTPS: File Transfer Protocol Secure

HTTP: Hyper Text Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

IP: Internet Protocol

SFTP: SSH File Transfer Protocol

SNMP: Simple Network Management Protocol

SSH: Secure Shell

Syslog: System Log

Web: World Wide Web

5 Technical Framework for Network Security Situation

Awareness

The technical framework for network security situation awareness mainly includes three parts:

front-end data sources, core components and other elements. Among them, the core components

of network security situation awareness are an important technical means to achieve the capability of network security situation awareness, which can be expressed in the form of

products, systems or platforms, or different functional components; achieving network security

chinastandards.org · PREVIEW

Preview: page 5 of 5 shown, 18 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-42453-2023