GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

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 People's Republic of China.

Table of Contents

Information Security Technology - General Technical Requirements for Network Security Situation Awareness

1 Scope

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.

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 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 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 situation awareness also relies on other elements, such as: emergency response, security decision-making and data sharing, etc. In order to better carry out network security situation awareness, the front-end data sources need to cover the communication network, regional boundaries and computing environment within the scope of network security situation awareness. This document stipulates the general technical requirements for the core components in the technical framework for network security situation awareness, excluding requirements for the relatively independent front-end data sources and other elements in the technical framework.

Based on the principle of universality and ensuring the functional completeness of network security situation awareness, the core components of network security situation awareness referred to in this document are composed of data aggregation, data analysis, situation display, monitoring and warning, data service interfaces and system management, etc., as shown in Figure 1, in which, the dashed box is not included in the technical requirements specified in this document. The data aggregation component collects data from corresponding front-end data sources in accordance with business demands, and stores it after pre-processing, such as: screening, conversion, completion and marking, etc., for subsequent data analysis. The data analysis component calls relevant data through the data service interfaces based on different data analysis models to conduct network attack analysis, asset risk analysis, abnormal behavior

For different front-end data sources, the data aggregation component shall support the following collection modes:

a) Passively receive data sent by the front-end data sources;

b) Actively initiate the acquisition of data from the front-end data sources, and support the setting of the data collection frequency;

c) Manually import data from the front-end data sources.

6.1.1.2 Collection protocols

The data aggregation component shall support two or more collection protocols for data collection in accordance with the application scenario. The collection protocols include, but are not limited to: Syslog, FTP/FTPS, SFTP, HTTP/HTTPS, SSH and SNMP, etc.

6.1.1.3 Collection content

The data aggregation component:

a) Shall support the collection of different types of data based on collection policies. The data types include: network traffic, asset information, logs, vulnerability information, user behavior, alarm information and threat information, etc.;

b) Shall support the customization of data types collected in accordance with the application scenario;

c) Shall support the utilization of verification technology or cryptography technology to ensure the integrity of data collected from the front-end data sources.

6.1.2 Data pre-processing

6.1.2.1 Data screening

The data aggregation component shall support the screening of collected original data based on data pre-processing rules, such as: removing data whose required fields are empty, removing data whose important fields are empty, removing data with incorrect data formats, and removing duplicate data, etc.

6.1.2.2 Data conversion

The data aggregation component shall support the conversion of collected original data of the same type and different formats into a unified data format, such as: a unified time format and a unified vulnerability name, etc. In addition, during the conversion, key data items must not be lost or damaged. The vulnerability description shall comply with the requirements of Chapter 5 of GB/T 28458-2020 and Chapter 5 and Chapter 6 of GB/T 30279-2020; the threat information description shall comply with the requirements of Chapter 6 of GB/T 36643-2018; the network attack description shall comply with the requirements of Chapter 6 and Chapter 7

of GB/T 37027-2018; the security incident description shall comply with the requirements of Chapter 5, Chapter 6 and Chapter 7 of GB/T 28517-2012.

6.1.2.3 Data completion

The data aggregation component shall support the completion of the collected original data based on the asset information database, threat information database and geographical information database, etc. The content of completion includes relevant attributes of asset, associated incidents and geographical locations, etc.

6.1.2.4 Data marking

The data aggregation component shall support the marking of collected original data in accordance with relevant data fields. The content of marking shall be set based on analysis demands, such as: data credibility and data source, etc.

6.1.3 Data storage

6.1.3.1 Data formats

The data aggregation component shall support the storage of structured, semi-structured and unstructured data.

6.1.3.2 Storage content

The data aggregation component:

a) Shall support the storage of business data, such as: collected traffic data, log data, alarm information, and generated security incidents and alarm information, etc.;

b) Shall support the storage of management data, such as: security policy data, running logs and operation logs, etc.;

c) Shall support the storage of knowledge data and the establishment of corresponding databases, such as: asset information database, geographical information database, attack signature database, vulnerability database, security incident database and threat information database, etc.

6.1.3.3 Storage time

The data aggregation component shall support the setting of storage time for various types of data.

6.1.3.4 Storage security

The data aggregation component shall support the integrity and confidentiality protection of stored important data and sensitive data, etc.

b) Shall support abnormal behavior analysis based on technologies, such as: behavior baselines, correlation analysis, data mining and machine learning, etc.;

c) Shall support the establishment of a profiling of user behaviors, including profiling of individual user behaviors and profiling of group behaviors;

d) Should support the learning to predict potential abnormal behaviors of users or entities based on historical data.

6.2.4 Security incident analysis

The data analysis component:

a) Shall support the classification and grading of security incidents based on asset importance, extent of harm caused and scope of impact;

b) Shall support the correlation analysis of asset-related threat information, network attack categories, network attack attributes and scope of impact, etc. based on security incidents;

c) Should support the combination of internal and external analytical capabilities to predict potential security incidents.

6.3 Requirements for Situation Display

6.3.1 Overall situation display

The situation display component:

a) Shall support the assessment and display of the overall security status of the network using scores or levels;

b) Shall support the assessment and display of local network security status of different industries, different regions, different business units or different assets using scores or levels;

c) Shall support the assessment and display of overall network security status over different time periods;

d) Shall support the utilization of multiple views to display the overall security situation. The display views include at least two of the following: radar chart, geographic information map, correlation diagram, threat path diagram, trend diagram, year-on-year / chain basis diagram, etc.;

e) Shall support role-based display, that is, display different contents for users in different roles;

f) Shall support the display of variation trends of the overall network security status, for

example, changes in scores or levels;

g) Shall support the assessment and display of different types of special situations in accordance with the application scenario.

6.3.2 Special situation display

6.3.2.1 Asset situation

The situation display component:

a) Shall support the graphical display of types and quantities of current assets;

b) Shall support the display of asset name, asset type, importance, IP address, open port and networking status, etc.

c) Shall support the assessment and display of the security status of assets, including the risk level of specific assets and the description of the security status of assets;

d) Shall support the display of variation trends of the security status of assets, such as: changes in asset risk levels and changes in networking status, etc.

6.3.2.2 Traffic situation

The situation display component:

a) Shall support the statistics and display of traffic data based on protocols, time, source IP address, destination IP address and front-end data sources, etc.;

b) Shall support the scope of statistics and display to at least include Internet traffic, specific user traffic and specific asset traffic, etc.;

c) Shall support the display of variation trends of traffic, such as: changes in the size of Internet traffic and changes in the size of front-end data source traffic, etc.

6.3.2.3 Operation situation

The situation display component:

a) Shall support the statistics and display of asset resource (such as: CPU, memory and network) usage;

b) Shall support the scope of statistics and display to at least include important assets and assets with abnormal operation, etc.;

c) Shall support the display of variation trends of asset resource usage, such as: changes in asset CPU / memory / network usage and changes in the quantity of assets with abnormal operation, etc.

d) Shall support the display of variation trends of abnormal behaviors of users or entities, such as: changes in abnormal behavior types and changes in abnormal behavior occurrence time, etc.

6.3.2.7 Security incident situation

The situation display component:

a) Shall support the display of security incidents found in the network, including incident time, incident type, incident name, incident level, incident object, attacker IP address, incident description and scope of impact, etc.;

b) Shall support the statistics and display of security incidents based on the quantity, type, level and asset distribution, etc. of security incidents;

c) Shall support the display of variation trends of security incidents, such as: changes in security incident types and changes in incident objects, etc.

6.3.3 Situation report

6.3.3.1 Data query

The situation display component:

a) Shall support the query of situation-related data;

b) Shall support combined queries based on time or other data fields;

c) Shall support sorting of query results in accordance with fields.

6.3.3.2 Statistical statement

The situation display component:

a) Shall support the generation and export of statistical statements based on the results of data analysis and situation assessment;

b) Shall support the generation of statistical statements or the generation of periodic statements based on a specified time period;

c) Shall support customized setting of statistical views and statement templates, and the use of multiple views to generate statistical statements.

6.3.3.3 Analysis report

The situation display component:

a) Shall support the generation and export of overall network security status analysis reports in accordance with data analysis results;

b) Shall support the generation and export of local network security status analysis reports of different regions and different business units in accordance with the data analysis results;

c) Shall support providing countermeasures or repair suggestions in accordance with the data analysis results;

d) Shall support the generation of analysis reports or the generation of periodic analysis reports based on a specified time period;

e) Shall support customized setting of templates of analysis reports.

6.4 Requirements for Monitoring and Warning

The monitoring and warning component:

a) Shall support the monitoring of network security status based on monitoring policies. The specific monitoring policy support can be customized in accordance with the application scenario;

b) Shall support level-based warning based on monitoring results and data analysis results, and in combination with warning rules;

c) Shall support warning in one or more of the following modes: platform, SMS, email and instant messaging, etc.;

d) Shall support the release of warning information in accordance with the warning level and warning process. The warning information includes, but is not limited to warning type, warning level, incident type, threat mode, involved objects, degree of impact and prevention countermeasures, etc.;

e) Shall support correlation analysis of affected assets through warning information, so as to obtain asset name, asset type and IP address, etc.;

f) Shall support the reporting of warning information. The reporting mode and content of warning information shall comply with relevant national regulations;

g) Should support linkage disposal with third-party equipment or systems based on warning information.

6.5 Requirements for Data Service Interfaces

6.5.1 Data exchange interface

The data service interface component:

a) Shall support data exchange with different front-end data sources, different internal modules and other external systems through interfaces. The data exchange includes,

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------