NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

GB/T 28454-2020

Information technology - Security techniques - Selection, deployment and operation of intrusion detection and prevention systems (IDPS)

Issued on: April 28, 2020 **Implemented on: November 1, 2020**

Issued by: SAMR; SAC

Table of Contents

Foreword

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

This standard replaces GB/T 28454-2012 "Information technology - Security techniques - Selection, deployment and operation of intrusion detection and prevention system (IDPS)". Compared with GB/T 28454-2012, the main technical changes are as follows.

- MODIFY the intrusion detection system IDS into the intrusion detection and prevention system (IDPS), bringing the intrusion prevention system IPS into the standard scope;
- MODIFY the scope of the standard, adding the applicable objects of the standard (see Chapter 1; Chapter 1 of the 2012 edition);
- MODIFY some terms and definitions, including "attack", "denial-of-service attack", "demilitarized zone", "intruder", "intrusion", "router", "switch", "Trojan horse", "attack signatures", "firewall", "host" "intrusion detection system", "intrusion prevention system", "provisioning", "detector", "test access point"; ADD some terms and definitions, including "distributed denial-of-service attack", "intrusion detection and prevention system", "virus" "virtual private network" "vulnerability" (see Chapter 3; Chapter 3 of the 2012 edition);
- ADD some abbreviations, including AIDPS, DMZ, DDoS, DoS, IDPS, I/O, IODEF, HIDPS, SIEM, VPN; DELETE the abbreviations NIDS and SIM (see Chapter 4; Chapter 4 of the 2012 edition);
- DELETE the introduction to the basic knowledge of IDPS in the background (see Chapter 5; Chapter 5 of the 2012 edition);
- Due to the addition of the intrusion prevention system, MODIFY that "When organizations have security level requirements for IDS products, see GB/T 20275" into that "When organizations have security level requirements for IDPS products, see GB/T 20275 and GB/T 28451." (See 7.3.1; 7.2 of the 2012 edition);
- ADD the considerations for IDPS selection in cloud computing environments (see

7.4.1, 7.4.2, 7.4.3, 7.4.5) and IDPS deployment methods in cloud environments, IDPS deployment methods in multi-level organizations, etc. (see 8.1);

- MODIFY the "Confirmation of capabilities" into "Verification of capabilities" (see 7.4.5; 7.3.5 in the 2012 version);

- MODIFY the SIEM function, adding the event correlation, event filtering, event aggregation (see 7.5.6; 7.4.6 of the 2012 version);

- DELETE the relevant content about the introduction of IDS and IPS in the response (see 9.5.2).

This standard uses the re-drafting method, to modify and adopt ISO/IEC 27039.2015 "Information technology - Security techniques - Selection, deployment and operations of intrusion detection and prevention systems (IDPS)".

Compared with ISO/IEC 27039.2015, this standard adds Chapter 2 "Normative references" and Chapter 4 "Abbreviations" to the structure; rearranges the contents of

7.3.1 and 7.3.2.

The technical differences between this standard and ISO/IEC 27039.2015 and their reasons are as follows.

- ADD Chapter 2 "Normative references" and Chapter 4 "Abbreviations", mainly to maintain continuity with GB/T 28454-2012;

- Delete the introduction to the basic knowledge of IDPS in the background of Chapter 3 (see Chapter 5), because this content is introduced in detail in Appendix A;

- ADD that "When there are security level requirements for IDPS products, see GB/T

20275 and GB/T 28451", which is mainly to consider the security level protection

requirements for IDPS products (see 7.3.1);

- DELETE the relevant content about IDS and IPS in 7.5.2 (see 9.5.2). Since it includes the intrusion prevention system IPS into the scope of this standard, and the standard object is defined as the intrusion detection and prevention system

IDPS, there is no need to introduce it separately;

- ADD the considerations for IDPS selection in cloud computing environments (see 7.4.1, 7.4.2, 7.4.3, 7.4.5), as well as IDPS deployment in cloud environments and IDPS deployment in multi-level organizations, mainly because the deployment of IDPS in the current cloud computing environment also needs to consider related matters, whilst international standards do not consider this part (see 8.1).

This standard has made the following editorial changes.

- DELETE note for 3.8.

Please note that some content in this document may be subject to patents. The publisher of this document assumes no responsibility for identifying these patents.

This standard was proposed by AND shall be under the jurisdiction of the National Information Security Standardization Technical Committee (SAC/TC 260).

Drafting organizations of this standard. Shandong Provincial Institute of Standardization, China Network Security Review Technology and Certification Center, Shaanxi Provincial Network and Information Security Evaluation Center, Beijing Tianrongxin Network Security Technology Co., Ltd., Shandong Chonghong Information Technology Co., Ltd., Chengdu Qinchuan IoT Technological Co., Ltd.

1 Scope

This standard gives guidance for organizations to deploy intrusion detection and prevention systems (IDPS). This standard details the selection, deployment, and operation of IDPS. This standard also provides the background information on which these guidelines are developed.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) is applicable to this standard.

GB/T 18336 (all parts) Information technology - Security techniques - Evaluation