INTERNATIONAL STANDARD

ISO/IEC 27039

First edition
2015-02-15

Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems (IDPS)

Technologies de l'information — Techniques de sécurité — Sélection, déploiement et opérations des systèmes de détection d'intrusion

Reference number
ISO/IEC 27039:2015(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword v
Introduction vi
1 Scope 1
2 Terms and definitions 1
3 Background 5
4 General 5
5 Selection 6
5.1 Introduction 6
5.2 Information security risk assessment 7
5.3 Host or Network IDPS 7
5.3.1 Overview 7
5.3.2 Host-based IDPS (HIDPS) 7
5.3.3 Network-based IDPS (NIDPS) 7
5.4 Considerations 8
5.4.1 System environment 8
5.4.2 Security protection mechanisms 8
5.4.3 IDPS security policy 8
5.4.4 Performance 9
5.4.5 Verification of capabilities 10
5.4.6 Cost 10
5.4.7 Updates 11
5.4.8 Alert strategies 12
5.4.9 Identity management 12
5.5 Tools that complement IDPS 13
5.5.1 Overview 13
5.5.2 File integrity checkers 14
5.5.3 Firewall 14
5.5.4 Honeypots 14
5.5.5 Network management tools 15
5.5.6 Security Information Event Management (SIEM) tools 15
5.5.7 Virus/Content protection tools 16
5.5.8 Vulnerability assessment tools 16
5.6 Scalability 17
5.7 Technical support 17
5.8 Training 18
6 Deployment 18
6.1 Overview 18
6.2 Staged deployment 18
6.3 NIDPS deployment 19
6.3.1 Overview 19
6.3.2 Location of NIDPS inside an Internet firewall 20
6.3.3 Location of NIDPS outside an Internet firewall 20
6.3.4 Location of NIDPS on a major network backbone 21
6.3.5 Location of NIDPS on critical subnets 21
6.4 HIDPS deployment 21
6.5 Safeguarding and protecting IDPS information security 22

7 Operations **22**
7.1 Overview 22
7.2 IDPS tuning 23
7.3 IDPS vulnerabilities 23
7.4 Handling IDPS alerts 23
7.4.1 Overview 23
7.4.2 Information Security Incident Response Team (ISIRT) 24
7.4.3 Outsourcing 24
7.5 Response options 25
7.5.1 Principles 25
7.5.2 Active response 25
7.5.3 Passive reaction 27
7.6 Legal Considerations 27
7.6.1 Overview 27
7.6.2 Privacy 27
7.6.3 Other legal and policy considerations 27
7.6.4 Forensics 27
Annex A (informative) **Intrusion Detection and Prevention System (IDPS): Framework and issues to be considered** **28**
Bibliography **48**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This first edition of ISO/IEC 27039 cancels and replaces ISO/IEC 18043:2006, which has been technically revised.

Legal notice

The National Institute of Standards and Technology (NIST), hereby grant non-exclusive license to ISO/IEC to use the NIST Special Publication on intrusion detection systems (SP800-94 rev1, July 2012) in the development of the ISO/IEC 27039 International Standard. However, the NIST retains the right to use, copy, distribute, or modify the SP800-94 as they see fit.

Introduction

Organizations should not only know when, if, and how an intrusion of their network, system, or application occurs. They also should know what vulnerability was exploited and what safeguards or appropriate risk treatment options (i.e. risk modification, risk retention, risk avoidance, risk sharing) should be implemented to prevent similar intrusions in the future. Organizations should also recognize and deter cyber-based intrusions. This requires an analysis of host and network traffic and/or audit trails for attack signatures or specific patterns that usually indicate malicious or suspicious intent. In the mid-1990s, organizations began to use intrusion detection and prevention systems (IDPS) to fulfil these needs. The general use of IDPS continues to expand with a wider range of IDPS products being made available to satisfy an increasing level of organizational demands for advanced intrusion detection capability.

In order for an organization to derive the maximum benefits from IDPS, the process of IDPS selection, deployment, and operations should be carefully planned and implemented by properly trained and experienced personnel. In the case where this process is achieved, then IDPS products can assist an organization in obtaining intrusion information and can serve as an important security device within the overall information and communications technology (ICT) infrastructure.

This International Standard provides guidelines for effective IDPS selection, deployment, and operation, as well as fundamental knowledge about IDPS. It is also applicable to those organizations that are considering outsourcing their intrusion detection capabilities. Information about outsourcing service level agreements can be found in the IT service management (ITSM) processes based on ISO/IEC 20000 Series.

This International Standard is intended to be helpful to:

a) An organization in satisfying the following requirements of ISO/IEC 27001:

- The organization shall implement procedures and other controls capable of enabling prompt detection of and response to security incidents;
- The organization shall execute monitoring and review procedures and other controls to properly identify attempted and successful security breaches and incidents.

b) An organization in implementing controls that meet the following security objectives of ISO/IEC 27002:

- To detect unauthorized information processing activities;
- Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified;
- An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities;
- System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

An organization should recognize that deploying IDPS is not a sole and/or exhaustive solution to satisfy or meet the above-cited requirements. Furthermore, this International Standard is not intended as criteria for any kind of conformity assessments, e.g., information security management system (ISMS) certification, IDPS services or products certification.

Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems (IDPS)

1 Scope

This International Standard provides guidelines to assist organizations in preparing to deploy intrusion detection and prevention systems (IDPS). In particular, it addresses the selection, deployment, and operations of IDPS. It also provides background information from which these guidelines are derived.

2 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

2.1
attack
attempts to destroy, expose, alter, or disable information systems and/or information within it or otherwise breach the security policy

2.2
attack signature
sequence of computing activities or alterations that are used to execute an attack and which are also used by an IDPS to discover that an attack has occurred and often is determined by the examination of network traffic or host logs

Note 1 to entry: This can also be referred to as an attack pattern.

2.3
attestation
variant of public-key encryption that lets IDPS software programs and devices authenticate their identity to remote parties

Note 1 to entry: See *remote attestation* (2.23).

2.4
bridge
network equipment that transparently connects a local area network (LAN) at OSI layer 2 to another LAN that uses the same protocol

2.5
cryptographic hash value
mathematical value that is assigned to a file and used to “test” the file at a later date to verify that the data contained in the file has not been maliciously changed

2.6
denial-of-service
DoS
unauthorized access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorized users

[SOURCE: ISO/IEC 27033-1:2009]