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)

COPYRIGHT PROTECTED DOCUMENT

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

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]

2.7
distributed denial-of-service attack
DDoS
unauthorized access to a system resource or the delaying of system operations and functions in the way of compromising multiple systems to flood the bandwidth or resources of the targeted system, with resultant loss of availability to authorized users

2.8
demilitarized zone
DMZ
logical and physical network space between the perimeter router and the exterior firewall

Note 1 to entry: The DMZ can be between networks and under close observation but does not have to be so.

Note 2 to entry: They are generally unsecured areas containing bastion hosts that provide public services.

2.9
exploit
defined way to breach the security of information systems through vulnerability

2.10
firewall
type of barrier placed between network environments — consisting of a dedicated device or a composite of several components and techniques — through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic as defined by the local security policy is allowed to pass

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

2.11
false positive
IDPS alert when there is no attack

2.12
false negative
no IDPS alert when there is an attack

2.13
honeypot
generic term for a decoy system used to deceive, distract, divert, and encourage the attacker to spend time on information that appears to be very valuable, but actually is fabricated and would not be of interest to a legitimate user

2.14
host
addressable system or computer in TCP/IP-based networks like the Internet

2.15
intruder
individual who is conducting, or has conducted, an intrusion or attack against a victim's host, site, network, or organization

2.16
intrusion
unauthorized access to a network or a network-connected system, that is, deliberate or accidental unauthorized access to information systems, to include malicious activity against information systems, or unauthorized use of resources within information systems

2.17
intrusion detection
formal process of detecting intrusions, generally characterized by gathering knowledge about abnormal usage patterns, as well as what, how, and which vulnerability has been exploited to include how and when it occurred

2.18
intrusion detection system
IDS
information systems used to identify that an intrusion has been attempted, is occurring, or has occurred

2.19
intrusion prevention system
IPS
variant on intrusion detection systems that are specifically designed to provide an active response capability

2.20
intrusion detection and prevention system
IDPS
intrusion detection systems (IDPS) and intrusion prevention systems (IPS) software applications or appliances that monitor systems for malicious activities, where IDS focus is to only alert on the discovery of such activity while IPS have the potent to prevent some intrusions upon detection

Note 1 to entry: IPS is deployed actively in the network if attack prevention is desired. If deployed in passive mode, it will not offer such functionality and effectively function as a regular IDS by providing alerts only.

2.21
penetration
unauthorized act of bypassing the security mechanisms of information systems

2.22
provisioning
process of loading the correct software, security policy, and configuration data for information technology (IT) devices

2.23
remote attestation
processes of using digital certificates to ensure the identity, as well as the hardware and software configuration, of IDPS and to securely transmit this information to a trusted operations centre

2.24
response
incident response or intrusion response
action taken to protect and restore the normal operational conditions of information systems and the information stored in it when an attack or intrusion occurs

2.25
router
network device that is used to establish and control the flow of data between different networks, by selecting paths or routes based upon routing protocol mechanisms and algorithms

Note 1 to entry: The networks can themselves be based on different protocols.

Note 2 to entry: The routing information is kept in a routing table.

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

2.26
server
computer system or program that provides services to other computers

2.27
Service Level Agreement
SLA
document that defines the technical support or business performance objectives including measures for performance and consequences for failure the provider of a service can provide its clients

2.28
sensor
component/agent of IDPS which collects event data from information systems or a network under observation

Note 1 to entry: Also referred to as a monitor.

2.29
subnet
segment of a network that shares a common address component

2.30
switch
device which provides connectivity between network connectivity devices by means of internal distribution mechanisms, with the switching technology typically implemented at layer 2 or layer 3 of the OSI reference model

Note 1 to entry: Switches are distinct from other local area network interconnection devices (e.g. a hub) as the technology used in switches sets up connections on a point-to-point basis.

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

2.31
test access port
TAP
typically passive devices that do not install any overhead on the network packet but also increase the level of the security as they make the data collection interface invisible to the network, where a switch can still maintain layer 2 information about the port

Note 1 to entry: A TAP also gives the functionality of multiple ports so network issues can be debugged without losing the IDPS capability.

2.32
trojan horse
malicious program that masquerades as a benign application

2.33
virus
type of malware which is software designed with malicious intent containing features or capabilities that can potentially cause harm, directly or indirectly, to the user and/or the user's system

2.34
virtual private network
VPN
restricted-use logical computer network that is constructed from the system resources of a physical network by using encryption and/or by tunnelling links of the virtual network across the real network

[SOURCE: ISO/IEC 18028-3:2005]

2.35
vulnerability
weakness of an asset or control that can be exploited by one or more threats

[SOURCE: ISO/IEC 27000:2012]

3 Background

The purpose of intrusion detection and prevention system (IDPS) is passively monitoring, detecting and logging inappropriate, incorrect, suspicious or anomalous activity that may represent an intrusion and provide an alert and/or an automated response when these activities are detected. It is the responsibility of the appointed IT Security personnel to actively review IDPS alerts and associated logs in order to make decisions on adequate responses. When an organization needs to detect promptly intrusions to the organization's information systems and responds appropriately to them, an organization should consider deploying IDPS. An organization can deploy IDPS by getting IDPS software and/or hardware products or by outsourcing capabilities of IDPS to an IDPS service provider.

There are many commercially available or open-source IDPS products and services that are based on different technologies and approaches. In addition, IDPS is not "plug and play" technology. Thus, when an organization is preparing to deploy IDPS, an organization should, as a minimum, be familiar with guidelines and information provided by this standard.

Fundamental knowledge about IDPS is mainly presented in Annex A. This annex explains the characteristics of different types of IDPS:

— Network-based, which monitors network traffic for particular network segments or devices and analyses the network and application protocol activity to identify suspicious activity;

— Host-based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity as well as three basic approaches for detection analysis, i.e. signature-based detection, statistical anomaly-based detection, stateful protocol analysis detection.

Behavioural analysis applies to network-based and host-based IDPS. This approach examines network traffic and host activities to identify threats that generate abnormal behaviour, such as distributed denial of service (DDoS) attacks, brute force attacks, certain forms of malware, and policy violations (e.g. a client system providing network services to other systems).

A host-based intrusion detection and prevention system (HIDPS) derives its source of information from one or more hosts, while a network-based intrusion and prevention system (NIDPS) derives its information from traffic of one or more network segments. The misuse-based approach models attacks on information systems as specific attack signatures, and then systematically scans the system for occurrences of these attack signatures. This process involves a specific encoding of previous behaviours and actions deemed intrusive or malicious. The anomaly-based approach attempts to detect intrusions by discovering significant deviations from normal behaviour on the assumption that attacks are different from normal/legitimate activity and can therefore be detected by systems that identify these differences.

An organization should understand that the source of information and the different analysis approaches may result in both advantages and disadvantages or limitations, which can impact the ability or inability to detect specific attacks and influence the degree of difficulty associated with installing and maintaining the IDPS.

4 General

IDPS functions and limitation, presented in Annex A, indicate that an organization should combine host-based (including application monitoring) and network-based approaches to achieve reasonably complete coverage of potential intrusions. Each type of IDPS has its strengths and limitations; together they can provide better security event coverage and alert analysis.

Combining the IDPS technologies depends on the availability of a correlation engine on the alert management system. Manual association of HIDPS and NIDPS alerts may result in IDPS operator overload without any additional benefit and the result may be worse than choosing the most appropriate output from one type of IDPS.

The process of selecting, deploying and operating IDPS within an organization is shown in Figure 1 along with the clauses that address the key steps in this process.

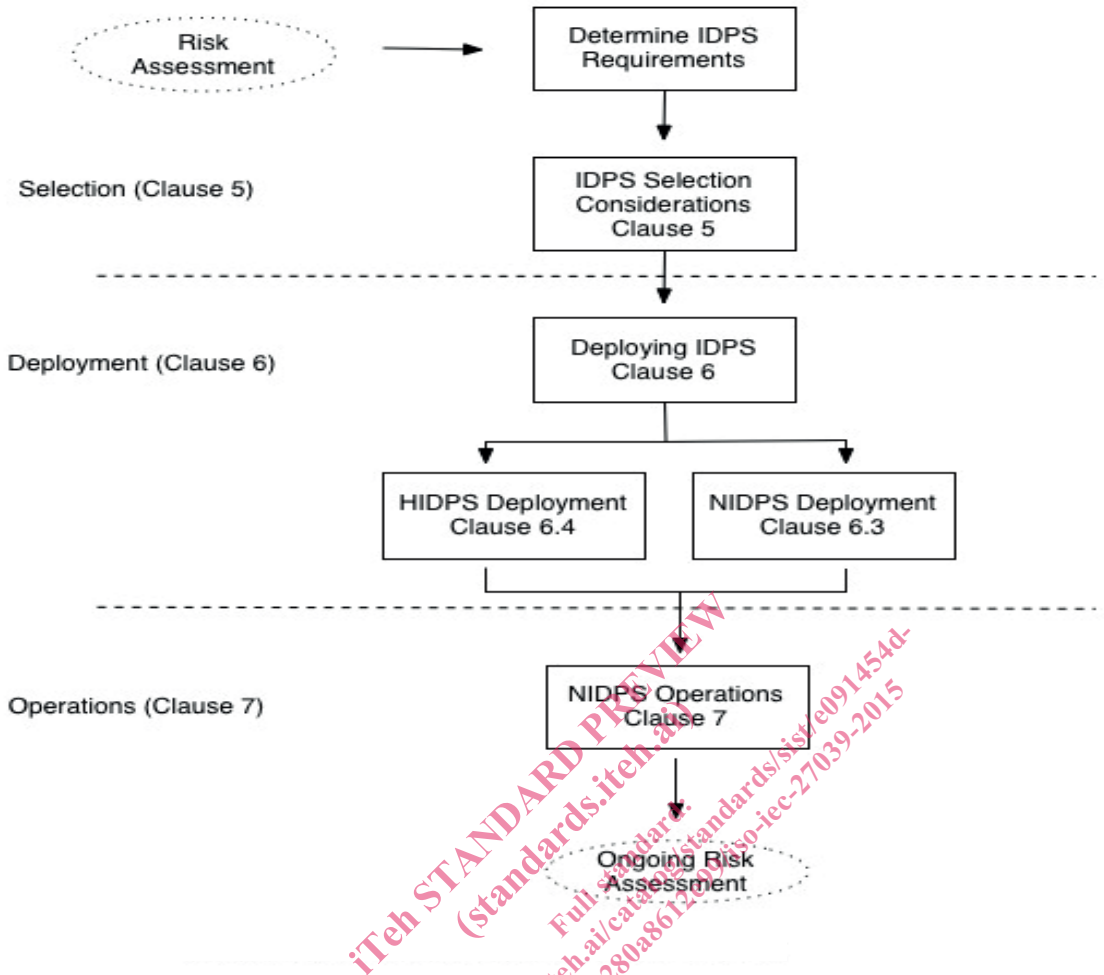

Figure 1 — Selection, deployment, and operations of IDPS

5 Selection

5.1 Introduction

There are many IDPS products and products families available. They range from extremely capable freeware offerings that can be deployed on a low-cost host to very expensive commercial systems requiring the latest hardware available. As there are so many different IDPS products to choose from, the process of selecting IDPS that represents the best fit for an organization's needs is difficult. Furthermore, there may be limited compatibility between various IDPS products offered in the market place. Additionally, because of mergers and the potentially wide geographical distribution of an organization, organizations may be forced to use different IDPS and the integration of these diverse IDPS can be very challenging.

Vendor brochures may not describe how well an IDPS can detect intrusions and how difficult it is to deploy, operate and maintain in an operational network with significant amounts of traffic. Vendors may indicate which attacks can be detected, but without access to an organization's network traffic, it is very difficult to describe how well the IDPS can perform and avoid false positives and negatives. Also the proactive and reactive capabilities of an IDPS need to be assessed independently and mapped to organizational requirements. This should include the need for deep packet inspection and reassembly versus the need for network performance and cost considerations. Consequently, relying on vendor provided information about IDPS capabilities is neither sufficient nor recommended.

ISO/IEC 15408 (all parts) may be used in the evaluation of an IDPS. In such a case, a document called "Security Target" may contain more accurate and reliable description than vendor brochures concerning IDPS performance. An organization should use this document in their selection process.

The following sub-clauses provide the major factors that should be used by an organization in the IDPS selection process.

5.2 Information security risk assessment

Prior to the selection of an IDPS, an organization should perform an information security risk assessment, aimed at identifying the attacks and intrusions (threats) to which the organization's specific information systems might be vulnerable, taking into account factors such as the nature of information used by the system and how it needs to be protected, the types of communication systems used, and other operational and environmental factors. By considering these potential threats in the context of their specific information security objectives, the organization can identify controls, which provide cost-effective mitigation of the risks. The identified controls would provide the basis of the requirements for the functions provided by their IDPS.

NOTE Information security risk assessment and management is the subject of International Standard (ISO/IEC 27001).

Once the IDPS is installed and operational an on-going process of risk management should be implemented to periodically review the effectiveness of the controls in light of changes to the system's operations and the threat environment.

5.3 Host or Network IDPS

5.3.1 Overview

IDPS deployment should be based on an organizational risk assessment and asset protection priorities. When selecting IDPS, the most effective method to monitor events should be investigated. Both Host-based IDPS (HIDPS) and Network-based (NIDPS) can be deployed in tandem. Where such an IDPS monitoring method is selected, an organization should implement it in stages starting with a NIDPS, as they are usually the simplest to install and maintain, then HIDPS should be deployed on critical servers.

Each option has its own advantages and disadvantages. For example, in the case where an IDPS is deployed outside an external firewall, an IDPS can generate a large number of alerts that do not require careful analysis because a large amount of the alerting events can indicate scans that are already being effectively prevented by the external firewall.

5.3.2 Host-based IDPS (HIDPS)

The choice of a HIDPS demands the identification of target hosts. The expensive nature of full-scale deployment on every host in an organization normally results in the deployment of HIDPS on critical hosts only. Therefore the deployment of HIDPS should be prioritized according to risk analysis results and cost-benefit considerations. An organization should deploy an IDPS capable of centralized management and reporting functions when HIDPS is deployed on all or a significant number of hosts.

5.3.3 Network-based IDPS (NIDPS)

The main factor to consider when deploying a NIDPS is where to position the system sensors. Options include:

— Inside external firewalls;

— Outside external firewalls;

— On major network backbones;

— Between trust boundaries.

