INTERNATIONAL STANDARD

ISO/IEC 18043

First edition
2006-06-15

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

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

Reference number
ISO/IEC 18043:2006(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

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18043 was prepared by Joint Technical Committee ISO/IEC JTC 1 *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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 (SP800-31) in the development of the ISO/IEC 18043 International Standard. However, the NIST retains the right to use, copy, distribute, or modify the SP800-31 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 transfer, risk acceptance, risk avoidance) should be implemented to prevent similar intrusions in the future. Organizations should also recognize and deflect 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 Systems (IDS) to fulfil these needs. The general use of IDS continues to expand with a wider range of IDS 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 IDS, the process of IDS 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 IDS 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 IDS selection, deployment and operation, as well as fundamental knowledge about IDS. 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.

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

1 Scope

This International Standard provides guidelines to assist organizations in preparing to deploy Intrusion Detection System (IDS). In particular, it addresses the selection, deployment and operations of IDS. It also provides background information from which these guidelines are derived.

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 17799:

- 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 IDS 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, IDS services or products certification.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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