ISO/IEC 18043:2006-06 (E)

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

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Terms and definitions 1

3 Background 4

4 General 5

5 Selection 6
5.1 Information Security Risk Assessment 7
5.2 Host or Network IDS 7
5.3 Considerations 7
5.4 Tools that complement IDS 13
5.5 Scalability 17
5.6 Technical support 17
5.7 Training 17

6 Deployment 18
6.1 Staged Deployment 18

7 Operations 22
7.1 IDS Tuning 22
7.2 IDS Vulnerabilities 22
7.3 Handling IDS Alerts 22
7.4 Response Options 25
7.5 Legal Considerations 26

Annex A (informative) Intrusion Detection System (IDS): Framework and Issues to be Considered ..27

A.1 Introduction to Intrusion Detection 27
A.2 Types of intrusions and attacks 28
A.3 Generic Model of Intrusion Detection Process 29
A.4 Types of IDS 35
A.5 Architecture 38
A.6 Management of an IDS 39
A.7 Implementation and Deployment Issues 42
A.8 Intrusion Detection Issues 44

Bibliography 46