

ISO/IEC 27039:2015-02 (E)

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

Contents		Page
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	15
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	18
5.8	Training	18
6	Deployment	18
6.1	Overview	18
6.2	Staged deployment	19
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