



<b>3</b>	<b>Application Intelligence and InterSpect .....</b>	<b>21</b>
	Objectives .....	21
	Key Terms .....	22
	The Need for Internal Security .....	24
	InterSpect and Perimeter Security .....	24
	Protecting Resource Value .....	25
	Legislation .....	25
	Threats and Protections .....	26
	Worms and Malware .....	26
	Patching .....	28
	External Countermeasures for Internal Resources .....	29
	Internal Controls .....	30
	InterSpect .....	33
	InterSpect Features .....	35
	SmartDefense .....	38
	Application Intelligence .....	38
	Components of SmartDefense .....	38
	SmartDefense Capabilities .....	39
	Implicit Defenses .....	39
	Abnormal-Behavior Analysis .....	40
	Subscription-Based Updates .....	40
	Web Intelligence .....	41
	Web Intelligence Components .....	41
	Centralized Control .....	42
	Online Updates .....	42
	Reapplying a SmartDefense Update .....	44
	Real-Time Attack Information .....	45
	Connection Blocking .....	46
	Network Segmentation .....	47
	Common Internal Attacks .....	49
	Worm Propagation .....	49
	Denial-of-Service (DoS) .....	50
	Distributed Denial-of-Service (DDoS) .....	50



<b>4</b>	<b>InterSpect Appliance Hardware .....</b>	<b>51</b>
	Objectives .....	51
	Key Terms .....	52
	InterSpect 210 .....	53
	Hardware Capabilities .....	53
	InterSpect 410/610/610F .....	58
	InterSpect 410 .....	58
	InterSpect 610 .....	58
	InterSpect 610F .....	59
	Hardware Capabilities .....	60
	Troubleshooting .....	67
	Mean Time Between Failures .....	67
<b>5</b>	<b>Configuring and Managing InterSpect .....</b>	<b>69</b>
	Objectives .....	69
	Key Terms .....	70
	Configuration and Setup .....	71
	Initial Configuration .....	71
	Basic Configuration .....	71
	Logging into SmartDashboard .....	72
	Managing InterSpect with SmartCenter Server .....	73
	Overview .....	73
	Understanding Central Management .....	73
	Secure Internal Communications (SIC) .....	74
	Performing a Central SmartDefense Update .....	75
	Centrally Managing an InterSpect Appliance .....	75
	InterSpect Logging .....	76

<b>6</b>	<b>Deployment Scenarios</b>	<b>77</b>
	Objectives	77
	Key Terms	78
	InterSpec Operational Overview	79
	Bridge Mode	80
	Switch Mode	81
	Router Mode	82
	Lab 1: InterSpec Configuration and Demonstration Toolkit Setup	85
	Lab 2: Configuring SecurePlatform Using sysconfig	89
	Lab 3: Accessing The InterSpec Web Interface	99
	Lab 4: Installing SmartDashboard	103
<b>7</b>	<b>SmartDefense and Web Intelligence</b>	<b>109</b>
	Objectives	109
	Key Terms	110
	SmartDashboard Tour	111
	General Information	113
	Zones	114
	Logging	117
	Dynamic Lists	120
	Switches	121
	Profiles	122
	Regular Expressions in InterSpec	125
	Protection Mechanisms	128
	Quarantine Configuration	128
	Network Security	129
	Application Intelligence	134
	Web Intelligence	157
	Web Servers	157
	Quarantine View	157
	Malicious Code	157
	Application Layer	158
	Information Disclosure	160



<b>8 InterSpect and Protocols .....</b>	<b>163</b>
Objectives .....	163
HTTP .....	164
HTTP Defined .....	164
Participants in an HTTP Session .....	164
InterSpect HTTP Protection Mechanisms .....	166
HTTP REQUEST Methods .....	166
HTTP Format Sizes .....	169
HTTP HEADERS (ASCII Only Requests) .....	170
HEADER REJECTION .....	170
HTTP on Non Standard Ports .....	171
Malicious HTTP Encodings .....	171
FTP .....	172
FTP Defined .....	172
The FTP Session .....	173
InterSpect FTP Protection Mechanisms .....	175
FTP Bounce Attack .....	175
CIFS Protocol .....	176
CIFS Defined .....	176
The CIFS Session .....	177
InterSpect CIFS Protection Mechanisms .....	179
File and Print Sharing: CIFS Worm .....	179
Null CIFS sessions .....	179
Blocking Popup Messages .....	179
Blocking ASN.1 Bitstring Encoding Attack .....	180
Blocking ASN.1 Bitstring Encoding Attacks over SMTP .....	180
Blocking Wins Replication Attack .....	181
Blocking WINS Name-Validation Attack .....	181
Blocking Long CIFS Passwords .....	181
Blocking SMB Server Buffer Overflows .....	182
Blocking Message-Queuing Buffer Overflows .....	182
P2P Protocol .....	183
The P2P Protocol Defined .....	183
Peer-to-peer networking sessions .....	183
SmartDefense P2P Protection Mechanisms .....	185
KaZaA .....	185



DirectConnect .....	186
Gnutella .....	186
eMule .....	187
BitTorrent .....	187
RPC Protocol .....	188
The RPC Protocol Defined .....	188
The RPC Session .....	189
SmartDefense RPC Protection Mechanisms .....	190
Unix-RPC .....	190
MS-RPC .....	191
Lab 5: Configuring InterSpect Bridge Mode .....	193
Lab Configuration .....	194
Lab 6: The InterSpect Demonstration Tool .....	209
<b>Appendix A: Updating SmartDefense .....</b>	<b>221</b>