Contents

Author Biography xi
Technical Editor Biography xiii
Foreword xv
Acknowledgments xvii

CHAPTER 1 Efficient Operations 1
Defining an Operations Center 1
Purpose of the Operations Center 3
Emergency Operations Center 4
Mission Operations Center 5
Threat Operations Center 5
Network Operations Center 5
Let Us Build a SOC! 6
Technology Phase 8
Organizational Phase 9
Policy Phase 9
Operational Phase 10
Intelligence Phase 10
Plan Your SOC 11
Logs 13
Event 16
Alerts 17
False Positive 18
True Positive 19
False Negative 19
True Negative 20
Incidents 20
Problems 22
Define Your Requirements 23
Summary 23

CHAPTER 2 Identify Your Customers 25
Internal Versus External Customers 27
Human Resources 27
Legal 28
Audit 29

Engineering/R&D 30
IT 30
External Customers 31
Customer Objectives 32
Service Level Agreements 32
Build and Document Your Use Cases 36
Use Case: Unauthorized Modification of User Accounts 38
Stakeholders: Compliance and Audit Departments 39
Use Case: Disabled User Account Reactivated 39
Stakeholders: HR and IT 39
Use Case: Any IDS Event that Scores Over a Severity of 7 40
Use Case: AV Failure 40
Stakeholders: Desktop Support Team, IT Server Management Teams 41
Use Case: Security Device Outage 41
Stakeholders: Security and IT 42
Use Case Rule Summary 42
Use Case: Top Vulnerabilities Detected in the Network 44
Stakeholders: Security, It, Audit, and Management 44
Use Case Reporting Summary 45
Expectations 46

CHAPTER 3 Infrastructure 49

Organizational Infrastructure > Operations Infrastructure > Support Infrastructure 51
Organizational Security Infrastructure 51
Perimeter Defenses 52
Network Defense 53
Host Defenses 53
Application Defenses 54
Data Defense 54
Policies and Procedures 54
Security Architecture 55
Siem/Log Management 56
Operation Center Infrastructure 59
- Ticketing Systems 59

Building the Ticket System 62
Subject 64
Parsed Values From Events 65
Time Ticket Created 66
User\Group\Queue 67

Source (SIEM, Email, Phone) 68
Category 69
Status 70
Reason Codes 70
Acknowledgment/Ticket Feedback 72
Workflow and Automation 73
Portal Interface 73
Mobile Devices 74
Support Infrastructure 74
Physical 75
Private SOC Network 80
Video Walls 81
Video Projectors 82
Labs 82

CHAPTER 4 Organizational Structure 85
Different Reporting Lines 88
Legal 89
CISO 90
CIO 91
Compliance 91
SOC Organization 92
Engineering 95
Security Architecture 96
Security Monitoring and Analysis 97
Responsibility 98
Authority 99
Fulfilling Needs 99

CHAPTER 5 Your Most Valuable Resource is Your People 101
Operational Security 104
Culture 105
Personality 106
Core Skill Sets 106
Analysts 109
Security Analyst—Job Description 110
Security Engineering 111
Security Operations Engineer—Job Description 112
Security Architect 114
Security Architect—Job Description 114

SOC Team Lead 115
SOC Team Lead—Job Description 116
SOC Management........ 117
SOC Manager—Job Description 118
SOC Games 120
Special Projects........ 123
Do Not Forget Your People........ 123

CHAPTER 6 Daily Operations........ 125
Problem and Change Event Communications 126
Master Station Logs 126
Shift Turn Overs 127
Daily Operations Calls........ 129
Critical Bridges........ 130
IR 134
Detection........ 134
Confirmation 134
Analysis 135
Containment........ 135
Recovery 136
Review 136
Communication Plan 137
Regular Workshops 138
Checklists........ 139
Shift Schedules 141
Types of Shift Schedules 143
Other Shift Options........ 146
Follow the Sun........ 146
Shift Rotation........ 147
Dealing with Absenteeism........ 148

CHAPTER 7 Training........ 151
Internal Functional Training........ 152
Internal Skill Set Training 154
Playbooks and Runbooks........ 154
Job Task Qualification Training........ 155
Tools and Product Training 155
Formal Training and Certifications........ 156
Schools and Universities........ 158
Vendor Training........ 158
OJT........ 159

Training Plans 160
SOC Shift Operations 161
Leaders 162
Customer Notifications 163
SOC Phones 163
Progression and Visibility 167
Training Exercises 168
Summary 171

CHAPTER 8 Metrics 173
Heads Up Display 174
Supervisor Metrics 175
Vulnerabilities 181
Vulnerability Prioritizing 184
Base CVSS2 Threshold 185
Temporal CVSS2 Threshold 185
Asset Prioritizing as a Part of Metrics 186
Historical Monitoring of Patches 190

CHAPTER 9 Intelligence 197
Know Thyself 200
Known IP Space, Know Thy Enemy 202
Blacklists 203
Black Listing Projects 208
Other Types of Lists 209
Organizations and Industry Partners 210
Proactive Activity Monitoring 213

CHAPTER 10 Outsourcing 215
Types of MSSPs 217
Strategic Partners 217
Pure Play Providers 217
Boutique Providers 218
Advantages of MSSP Outsourcing 219
Cost 220
Organizational 221
Enhanced Capabilities 221
SLA 222
Documentation 223
Disadvantages to MSSP Outsourcing 224
Large Numbers of Customers 224