
Table of Contents

Foreword.....	ix
---------------	----

Preface.....	xiii
--------------	------

Part I. The Fundamentals

1. Introduction.....	1
Intelligence as Part of Incident Response	1
History of Cyber Threat Intelligence	1
Modern Cyber Threat Intelligence	2
The Way Forward	3
Incident Response as a Part of Intelligence	4
What Is Intelligence-Driven Incident Response?	5
Why Intelligence-Driven Incident Response?	5
Operation SMN	5
Operation Aurora	6
Conclusion	7
2. Basics of Intelligence.....	9
Data Versus Intelligence	10
Sources and Methods	11
Process Models	14
OODA	14
Intelligence Cycle	17
Using the Intelligence Cycle	21
Qualities of Good Intelligence	23
Levels of Intelligence	24

Tactical Intelligence	24
Operational Intelligence	24
Strategic Intelligence	25
Confidence Levels	25
Conclusion	26
3. Basics of Incident Response.....	27
Incident-Response Cycle	28
Preparation	28
Identification	30
Containment	30
Eradication	31
Recovery	32
Lessons Learned	33
Kill Chain	35
Targeting	36
Reconnaissance	37
Weaponization	38
Delivery	42
Exploitation	43
Installation	43
Command and Control	44
Actions on Objective	45
Example Kill Chain	47
Diamond Model	49
Basic Model	49
Extending the Model	50
Active Defense	50
Deny	51
Disrupt	51
Degrade	52
Deceive	52
Destroy	52
F3EAD	53
Find	54
Fix	54
Finish	54
Exploit	55
Analyze	55
Disseminate	55
Using F3EAD	56
Picking the Right Model	57

Scenario: GLASS WIZARD	57
Conclusion	58

Part II. Practical Application

4. Find.....	61
Actor-Centric Targeting	62
Starting with Known Information	63
Useful Find Information	64
Asset-Centric Targeting	70
Using Asset-Centric Targeting	71
News-Centric Targeting	71
Targeting Based on Third-Party Notification	72
Prioritizing Targeting	73
Immediate Needs	74
Past Incidents	74
Criticality	74
Organizing Targeting Activities	75
Hard Leads	75
Soft Leads	75
Grouping Related Leads	75
Lead Storage	76
The Request for Information Process	77
Conclusion	77
5. Fix.....	79
Intrusion Detection	80
Network Alerting	80
System Alerting	85
Fixing GLASS WIZARD	87
Intrusion Investigation	89
Network Analysis	89
Live Response	96
Memory Analysis	96
Disk Analysis	97
Malware Analysis	99
Scoping	101
Hunting	102
Developing Leads	102
Testing Leads	103
Conclusion	103

6. Finish.....	105
Finishing Is <i>Not</i> Hacking Back	105
Stages of Finish	106
Mitigate	107
Remediate	109
Rearchitect	112
Taking Action	113
Deny	113
Disrupt	114
Degrade	115
Deceive	115
Destroy	116
Organizing Incident Data	116
Tools for Tracking Actions	117
Purpose-Built Tools	119
Assessing the Damage	120
Monitoring Life Cycle	121
Conclusion	122
7. Exploit.....	123
What to Exploit?	124
Gathering Information	125
Storing Threat Information	126
Data Standards and Formats for Indicators	126
Data Standards and Formats for Strategic Information	130
Managing Information	132
Threat-Intelligence Platforms	133
Conclusion	135
8. Analyze.....	137
The Fundamentals of Analysis	137
What to Analyze?	139
Conducting the Analysis	141
Enriching Your Data	142
Developing Your Hypothesis	146
Evaluating Key Assumptions	147
Judgment and Conclusions	151
Analytic Processes and Methods	151
Structured Analysis	151
Target-Centric Analysis	154
Analysis of Competing Hypotheses	156
Graph Analysis	158

Contrarian Techniques	159
Conclusion	161
9. Disseminate.....	163
Intelligence Consumer Goals	164
Audience	164
Executive/Leadership Consumer	165
Internal Technical Consumers	167
External Technical Consumers	169
Developing Consumer Personas	170
Authors	173
Actionability	174
The Writing Process	176
Plan	176
Draft	177
Edit	178
Intelligence Product Formats	180
Short-Form Products	180
Long-Form Products	184
The RFI Process	193
Automated Consumption Products	197
Establishing a Rhythm	202
Distribution	202
Feedback	203
Regular Products	203
Conclusion	204

Part III. The Way Forward

10. Strategic Intelligence.....	207
What Is Strategic Intelligence?	208
Developing Target Models	209
The Strategic Intelligence Cycle	212
Setting Strategic Requirements	212
Collection	213
Analysis	216
Dissemination	220
Conclusion	220
11. Building an Intelligence Program.....	223
Are You Ready?	223

Planning the Program	225
Defining Stakeholders	226
Defining Goals	227
Defining Success Criteria	228
Identifying Requirements and Constraints	228
Defining Metrics	230
Stakeholder Personas	230
Tactical Use Cases	231
SOC Support	232
Indicator Management	232
Operational Use Cases	234
Campaign Tracking	234
Strategic Use Cases	235
Architecture Support	235
Risk Assessment/Strategic Situational Awareness	236
Strategic to Tactical or Tactical to Strategic?	237
Hiring an Intelligence Team	238
Demonstrating Intelligence Program Value	238
Conclusion	239
A. Intelligence Products.....	241
Index.....	251