Table of Contents

COURSE WORKBOOK

Domain 01
Overview of The Incident Response Life Cycle 08

Domain 02
Understanding the Threat Landscape 13

Domain 03
Building an Effective Incident Response Capability 22

Domain 04
Preparing for Incident Response Investigations 29

Domain 05
Vulnerability Assessment and Management 34

Domain 06
Identifying Network and System Baselines 39

Domain 07
Indicators of Compromise and Threat Identification 44

Domain 08
Investigative Principles and Lead Development 50

Domain 09
Threat Intelligence Collection and Analysis 54

Domain 10
Overview of Data Forensics and Analysis 63

Domain 11
Host-Based Data Collection Practices 70

Domain 12
Network-Based Data Collection Practices 76

Domain 13
Static and Dynamic Malware Triage 83

Domain 14
Incident Containment and Remediation 89

Domain 15
Incident Reporting and Lessons Learned 101

Domain 16
Creating Playbooks and Response Scenarios 106

WIRESHARK LAB EXERCISES **113**

Lab Exercise 01
Personalizing Your Virtual Machine 115

Lab Exercise 02
The Wireshark User Interface 129

Lab Exercise 03
Customizing Wireshark Settings 137

Lab Exercise 04
Applying Capture Filters 147

Lab Exercise 05
Applying Display Filters 157

Lab Exercise 06
Color Rules and Packet Export 167

Lab Exercise 07
Creating Tables and Graphs 179

Lab Exercise 08
File and Object Reassembly 189

Lab Exercise 09
Adding Comments to Trace Files 197

Lab Exercise 10
Command-Line Capture Tools 205

STUDENT REFERENCE GUIDE **217**

NIST Special Publication 800-61
Computer Security Incident Handling Guide 219