Contents

Foreword VII

Preface IX

1 Introduction
Marcus A. Maloof 1

Part I Survey Contributions

2 An Introduction to Information Assurance
Clay Shields 7

3 Some Basic Concepts of Machine Learning and Data Mining
Marcus A. Maloof 23

Part II Research Contributions

4 Learning to Detect Malicious Executables
Jeremy Z. Kolter, Marcus A. Maloof 47

5 Data Mining Applied to Intrusion Detection: MITRE Experiences
Eric E. Bloedorn, Lisa M. Talbot, David D. DeBarr 65

6 Intrusion Detection Alarm Clustering
Klaus Julisch 89

7 Behavioral Features for Network Anomaly Detection
James P. Early, Carla E. Brodley 107

8 Cost-Sensitive Modeling for Intrusion Detection
Wenke Lee, Wei Fan, Salvatore J. Stolfo, Matthew Miller 125

9 Data Cleaning and Enriched Representations for Anomaly Detection in System Calls
Gaurav Tandon, Philip Chan, Debasis Mitra 137

10 A Decision-Theoretic, Semi-Supervised Model for Intrusion Detection
Terran Lane 157

References 179

Index 199

http://www.springer.com/978-1-84628-029-0

Machine Learning and Data Mining for Computer Security
Methods and Applications
Maloof, M.A. (Ed.)
2006, XVI, 210 p., Hardcover
ISBN: 978-1-84628-029-0