1. Record Nr. UNINA9910632494403321

Autore	Xu Shengjie
Titolo	Cybersecurity in Intelligent Networking Systems
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2022 ©2023
ISBN	1-119-78413-1 1-119-78410-7 1-119-78412-3
Descrizione fisica	1 online resource (147 pages)
Collana	IEEE Press Ser.
Altri autori (Persone)	QianYi HuRose Qingyang
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Title Page -- Copyright -- Contents -- About the Authors -- Preface -- Acknowledgments -- Acronyms -- Chapter 1 Cybersecurity in the Era of Artificial Intelligence -- 1.1 Artificial Intelligence for Cybersecurity -- 1.1.1 Artificial Intelligence -- 1.1.2 Machine Learning -- 1.1.2.1 Supervised Learning -- 1.1.2.2 Unsupervised Learning -- 1.1.2.3 Semisupervised Learning -- 1.1.2.4 Reinforcement Learning -- 1.1.3 DataDriven Workflow for Cybersecurity -- 1.2 Key Areas and Challenges -- 1.2.1 Anomaly Detection -- 1.2.2 Trustworthy Artificial Intelligence -- 1.2.3 Privacy Preservation -- 1.3 Toolbox to Build Secure and Intelligent Systems -- 1.3.1 Machine Learning and Deep Learning -- 1.3.1.1 NumPy -- 1.3.1.2 SciPy -- 1.3.1.3 Scikitlearn -- 1.3.1.4 PyTorch -- 1.3.1.5 TensorFlow -- 1.3.2 PrivacyPreserving Machine Learning -- 1.3.2.1 Syft -- 1.3.2.2 TensorFlow Federated -- 1.3.2.3 TensorFlow Privacy -- 1.3.3 Adversarial Machine Learning -- 1.3.3.1 SecML and SecML Malware -- 1.3.3.2 Foolbox -- 1.3.3.3 CleverHans -- 1.3.3.4 Counterfit -- 1.3.3.5 MintNV -- 1.4 Data Repositories for Cybersecurity Research -- 1.4.1 NSLKDD -- 1.4.2 UNSWNB15 -- 1.4.3 EMBER -- 1.5 Summary -- Notes -- References -- Chapter 2 Cyber Threats and Gateway Defense -- 2.1 Cyber Threats -- 2.1.1 Cyber Intrusions -- 2.1.2 Distributed Denial of Services Attack --