1. Record Nr. UNISA996499857703316

Autore	Neshenko Nataliia
Titolo	Smart cities : cyber situational awareness to support decision making / / Nataliia Neshenko, Elias Bou-Harb, and Borko Furht
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-18464-5
Descrizione fisica	1 online resource (134 pages)
Disciplina	005.8
Soggetti	Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Intro -- Preface -- What Is Covered in This Book? -- Contents -- Part I Cybersecurity of Smart City -- 1 Rise of Smart Cities -- 1.1 Forces of Change -- 1.2 Set the Scene for Smart City -- 1.2.1 What Make City Smart? -- 1.2.2 Dimensions of Smart City -- 1.2.2.1 Physical Tier -- 1.2.2.2 Technological Tier -- 1.2.2.3 Analytical Tier -- 1.2.2.4 Operational Tier -- 1.2.2.5 Management Tier -- 1.2.2.6 Stakeholder Tier -- 1.3 Summary -- References -- 2 Cyber Brittleness of Smart Cities -- 2.1 Cybersecurity of Smart Cities vs Enterprise IT Security -- 2.2 Cyber Incidents: Decades in Retrospect -- 2.2.1 The Colonial Pipeline Attack -- 2.2.2 Israel's Water System Attack -- 2.2.3 Onslow Water and Sewer Company Hack -- 2.2.4 Battle of City Atlanta -- 2.2.5 Kemuri Water Company -- 2.2.6 Ukraine Power Grid Attack -- 2.2.7 German Steel Mill Attack -- 2.2.8 The Cyber-Attack on Saudi Aramco -- 2.3 Adversary Model -- 2.3.1 Attackers -- 2.3.2 Impact of Cyber-Attacks -- 2.3.3 Categorization of Cyber Threats -- 2.3.3.1 Discovery Threats -- 2.3.3.2 Infrastructure Threats -- 2.3.3.3 Data Threats -- 2.3.3.4 Third-Party Vulnerability -- 2.4 Summary -- References -- Part II Cyber Situational Awareness for Smart City -- 3 Cyber Situational Awareness Frontiers -- 3.1 Toward Analytics-Driven Situational Awareness -- 3.1.1 Data Analytical Techniques -- 3.1.1.1 Machine Learning and Data Mining Methods -- 3.1.1.2 Knowledge-Based Models -- 3.1.2 Threat Perception: Attack Detection Methods -- 3.1.3 Evaluation Metrics -- 3.1.4 Threat Comprehension: Risk Analysis and

Cyber Threat Intelligence -- 3.1.5 Risk Analysis -- 3.1.6 Cyber Threat Intelligence -- 3.1.7 Threat Projection: Strategies for Modeling Cascading Effect -- 3.2 Analytics-Driven Cyber Situational Awareness for Smart City: Are We There Yet? -- 3.2.1 Toward Threat Coverage -- 3.2.2 Toward Human Cognition Engagement.
3.2.3 Toward Data Availability -- 3.3 Summary -- References -- 4 Cyber Situational Awareness for Industrial Control Systems (ICSs) Deployed in Smart City -- 4.1 Development of Successful Situational Awareness Program -- 4.1.1 Plan for Situational Awareness -- 4.1.2 Collect and Analyze Relevant Data -- 4.1.3 Communicate to Make Appropriate Decisions -- 4.1.4 Enhance Process and Technology -- 4.2 Framework Overview -- 4.2.1 Design Considerations -- 4.2.2 Detailed Design -- 4.2.2.1 Module 1: Behavior Fingerprinting -- 4.2.2.2 Module 2: Attack Inference -- 4.2.2.3 Module 3: Attack Localization -- 4.2.2.4 Module 4: Impact Assessment -- 4.2.2.5 Module 5: Interactive Visualization -- 4.3 Continuous Improvement: Evaluation Strategy -- 4.4 Summary -- References -- 5 Case Study: Situational Awareness for Water Treatment Systems -- 5.1 History of Attacks Against Water Infrastructure -- 5.1.1 Israel's Water System Attack -- 5.1.2 Onslow Water and Sewer Company Hack -- 5.1.3 Kemuri Water Company -- 5.1.4 The Maroochy Water Services Attack -- 5.2 Cyber Situation Awareness for Water Treatment Plant -- 5.2.1 Cyber-Physical Process Overview -- 5.2.2 Dataset Overview -- 5.2.2.1 Attack Scenarios -- 5.2.3 Operational Patterns Examination -- 5.2.4 Cyber Incident Detection -- 5.2.5 Anomaly Localization -- 5.2.6 Interactive Visualization -- 5.3 Summary -- References -- 6 Looking Ahead: Future Perspectives and Opportunities of Cyber Situational Awareness for Smart Cities -- 6.1 Challenges and Future Perspective -- 6.2 Summary -- References.