River Publishers Series in Digital Security and Forensics

Developing a Cybersecurity Immune System for Industry 4.0

Authors:
Sergei Petrenko, Innopolis University, Russia
ISBN: 9788770221887
e-ISBN: 9788770221870
Available From: June 2020
Price: € 95.00

Description:

Cyber immune systems try to mimic the adaptive immune system of humans and animals because of its capability to detect and fend off new, unseen pathogens. Today's current cyber security systems provide an effective defense mechanism against known cyber-attacks but are not so good when it comes to defending against unknown attacks. This book describes the possible development and organization of self-healing computing based on cyber immunity techniques and aimed at working in the new realm of Industry 4.0. Industry 4.0 is the trend towards automation and data exchange in manufacturing technologies and processes which include cyber-physical systems (CPS), the internet of things (IoT), industrial internet of things (IIOT), cloud computing, cognitive computing and artificial intelligence. The book describes the author's research and development of cyber-immunity systems that will prevent the destruction of critical information infrastructure by future unknown cyber-attacks and thus avoid the significant or catastrophic consequences of such attacks. The book is designed for undergraduate and post-graduate students, for engineers in related fields as well as managers of corporate and state structures, chief information officers (CIO), chief information security officers (CISO), architects, and research engineers in the field of cybersecurity.

This book contains four chapters

- Cyber Immunity Concept of the Industry 4.0;
- Mathematical Framework for Immune Protection of Industry 4.0;
- Trends and prospects of the development of Immune Protection of Industry 4.0;
- From detecting cyber-attacks to self-healing Industry 4.0;

Keywords: Computer Immunology, Immune Response, “Friend or Foe”, Danger Theory, Immuno-computing, Hybrid Intelligent Cybersecurity Systems, Self-healing Computing, Cyber Immunity of Industry 4.0, ?yber-Resilience, ?yber-Security, Group and Mass Cyber-attacks, Digital Economy, Critical Information Infrastructure, New models and methods for collecting and processing big data (Big Data) and streaming data processing (ETL), In-Depth Knowledge (Deep Learning), Semantic and Cognitive Analysis (Computational Cognitivism).