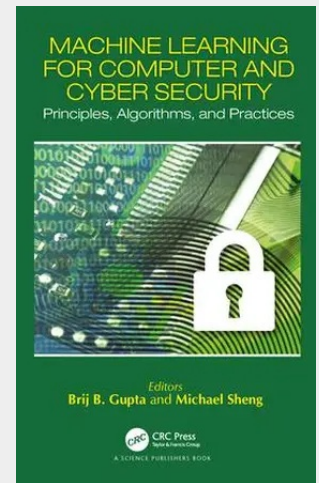


Machine Learning for Computer and Cyber Security

Principle, Algorithms, and Practices

While Computer Security is a broader term which incorporates technologies, protocols, standards and policies to ensure the security of the computing systems including the computer hardware, software and the information stored in it, Cyber Security is a specific, growing field to protect computer networks (offline and online) from unauthorized access, botnets, phishing scams, etc. Machine learning is a branch of Computer Science which enables computing machines to adopt new behaviors on the basis of observable and verifiable data and information. It can be applied to ensure the security of the computers and the information by detecting anomalies using data mining and other such techniques. This book will be an invaluable resource to understand the importance of machine learning and data mining in establishing computer and cyber security. It emphasizes important security aspects associated with computer and cyber security along with the analysis of machine learning and data mining based solutions. The book also highlights the future research domains in which these solutions can be applied. Furthermore, it caters to the needs of IT professionals, researchers, faculty members, scientists, graduate students, research scholars and software developers who seek to carry out research and develop combating solutions in the area of cyber security using machine learning based approaches. It is an extensive source of information for the readers belonging to the field of Computer Science and Engineering, and Cyber Security professionals. Key Features: - This book contains examples and illustrations to demonstrate the principles, algorithms, challenges and applications of machine learning and data mining for computer and cyber security. - It showcases important security aspects and current trends in the field. - It provides an insight of the future research directions in the field. - Contents of this book help to prepare the students for exercising better defense in terms of understanding the motivation of the attackers and how to deal with and mitigate the situation using machine learning based approaches in better manner.

While Computer Security is a broader term which incorporates technologies, protocols, standards and policies to ensure the security of the computing systems including the computer hardware, software and the information stored in it, Cyber Security is a specific, growing field to protect computer networks (offline and online) from unauthorized access, botnets, phishing scams, etc. Machine learning is a branch of Computer Science which enables computing machines to adopt new behaviors on the basis of observable and verifiable data and information. It can be applied to ensure the security of the computers and the information by detecting anomalies using data mining and other such techniques. This book will be an invaluable resource to understand the importance of machine learning and data mining in establishing computer and cyber security. It emphasizes important security aspects associated with computer and cyber security along with the analysis of machine learning and data mining based solutions. The book also highlights the future research domains in which these solutions can be applied. Furthermore, it caters to the needs of IT professionals, researchers, faculty members, scientists, graduate students, research scholars and software developers who seek to carry out research and develop combating solutions in the area of cyber security using machine learning based approaches. It is an extensive source of information for the readers belonging to the field of Computer Science and Engineering, and Cyber Security professionals. Key Features: - This book contains examples and illustrations to demonstrate the principles, algorithms, challenges and applications of machine learning and data mining for computer and cyber security. - It showcases important security aspects and current trends in the field. - It provides an insight of the future research directions in the field. - Contents of this book help to prepare the students for exercising better defense in terms of understanding the motivation of the attackers and how to deal with and mitigate the situation using machine learning based approaches in better manner.



258,50 €

258,50 € (zzgl. MwSt.)

Nicht mehr lieferbar

Artikelnummer: 9781138587304

Medium: Buch

ISBN: 978-1-138-58730-4

Verlag: CRC Press

Erscheinungstermin: 13.02.2019

Sprache(n): Englisch

Auflage: 1. Auflage 2019

Serie: Cyber Ecosystem and Security

Produktform: Gebunden

Gewicht: 771 g

Seiten: 352

Format (B x H): 163 x 234 mm

