

1. Record Nr.	UNINA9910254359303321
Titolo	Information Fusion for Cyber-Security Analytics // edited by Izzat M Alsmadi, George Karabatis, Ahmed Aleroud
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-44257-0
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (X, 379 p. 85 illus., 61 illus. in color.)
Collana	Studies in Computational Intelligence, , 1860-949X ; ; 691
Disciplina	005.8
Soggetti	Electrical engineering Electronic circuits Computer security Big data Communications Engineering, Networks Circuits and Systems Systems and Data Security Big Data/Analytics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Introduction -- Part 1: Information Fusion for Cyber-Security Analytics -- Activity Information Fusion for Security Analytics -- Location Information Fusion for Security Analytics -- Time Information Fusion for Security Analytics -- Individuality Information Fusion for Security Analytics -- Relation Information Fusion for Security Analytics -- Part 2: Trends in Using Information Fusion Techniques to Discover Cyber Threats -- Big Data Fusion for Predicting Network Threats -- Using Software Defined Networks for Cyber Threat Discovery -- Privacy Preserving Information Fusion for Analyzing Network Data -- Using Information Fusion to Discover Zero-Day Attacks -- Enhancing Social Network Privacy and Security Using Graph-based Data Fusion -- Using Information Fusion to discover Cyber-threats in Wireless Sensor Networks -- Information Fusion for Improving Privacy and Security in Healthcare Applications -- Predicting Social Engineering Attacks Using Information Fusion Techniques -- Part 3: Applications and tools. -

This book highlights several gaps that have not been addressed in existing cyber security research. It first discusses the recent attack prediction techniques that utilize one or more aspects of information to create attack prediction models. The second part is dedicated to new trends on information fusion and their applicability to cyber security; in particular, graph data analytics for cyber security, unwanted traffic detection and control based on trust management software defined networks, security in wireless sensor networks & their applications, and emerging trends in security system design using the concept of social behavioral biometric. The book guides the design of new commercialized tools that can be introduced to improve the accuracy of existing attack prediction models. Furthermore, the book advances the use of Knowledge-based Intrusion Detection Systems (IDS) to complement existing IDS technologies. It is aimed towards cyber security researchers. .