1.	Record Nr.	UNINA9910463628803321
	Titolo	Information security analytics : finding security insights, patterns and anomalies in big data / / Mark Talabis [and three others] ; D. Kaye, technical editor
	Pubbl/distr/stampa	Waltham, Massachusetts : , : Syngress, , 2015 ©2015
	ISBN	0-12-800506-8
	Edizione	[1st edition]
	Descrizione fisica	1 online resource (183 p.)
	Disciplina	005.8
	Soggetti	Computer security Information resources management - Security measures Big data - Security measures Electronic books.
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
	Nota di contenuto	Front Cover; Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data; Copyright; Dedication; Contents; Foreword; About the Authors; Acknowledgments; Chapter 1 - Analytics Defined; INTRODUCTION TO SECURITY ANALYTICS; CONCEPTS AND TECHNIQUES IN ANALYTICS; DATA FOR SECURITY ANALYTICS; ANALYTICS IN EVERYDAY LIFE; SECURITY ANALYTICS PROCESS; REFERENCES; Chapter 2 - Primer on Analytical Software and Tools; STATISTICAL PROGRAMMING; INTRODUCTION TO DATABASES AND BIG DATA TECHNIQUES; REFERENCES; Chapter 3 - Analytics and Incident Response; INTRODUCTION SCENARIOS AND CHALLENGES IN INTRUSIONS AND INCIDENT IDENTIFICATIONANALYSIS OF LOG FILES; LOADING THE DATA; ANOTHER POTENTIAL ANALYTICAL DATA SET: UNSTACKED STATUS CODES; OTHER APPLICABLE SECURITY AREAS AND SCENARIOS; SUMMARY; FURTHER READING; Chapter 4 - Simulations and Security Processes; SIMULATION; CASE STUDY; Chapter 5 - Access Analytics; INTRODUCTION; TECHNOLOGY PRIMER; SCENARIO, ANALYSIS, AND TECHNIQUES; CASE STUDY; ANALYZING THE RESULTS; Chapter 6 -

Sommario/riassunto

Information Security Analytics gives you insights into the practice of analytics and, more importantly, how you can utilize analytic techniques to identify trends and outliers that may not be possible to identify using traditional security analysis techniques.   Information Security Analytics dispels the myth that analytics within the information security domain is limited to just security incident and event management systems and basic network analysis. Analytic techniques can help you mine data and identify patterns and relationships in any form of security data. Using the techniques covere