

1. Record Nr.	UNINA9910993931003321
Autore	Beuran Razvan
Titolo	Cybersecurity Education and Training // by Razvan Beuran
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025
ISBN	9789819605552 9819605555
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XVI, 323 p. 28 illus.)
Disciplina	005.8
Soggetti	Computer security Principles and Models of Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Overview of cybersecurity education and training -- Technical cybersecurity training -- Attack training -- Forensics training -- Defense training -- Security awareness training -- Cybersecurity training platforms -- Case study: Cytrone -- Case study: Kypo -- Training platform capability assessment -- Conclusion.
Sommario/riassunto	This book provides a comprehensive overview on cybersecurity education and training methodologies. The book uses a combination of theoretical and practical elements to address both the abstract and concrete aspects of the discussed concepts. The book is structured into two parts. The first part focuses mainly on technical cybersecurity training approaches. Following a general outline of cybersecurity education and training, technical cybersecurity training and the three types of training activities (attack training, forensics training, and defense training) are discussed in detail. The second part of the book describes the main characteristics of cybersecurity training platforms, which are the systems used to conduct the technical cybersecurity training activities. This part includes a wide-ranging analysis of actual cybersecurity training platforms, namely Capture The Flag (CTF) systems and cyber ranges that are currently being used worldwide, and a detailed study of an open-source cybersecurity training platform, CyTrONE. A cybersecurity training platform capability assessment methodology that makes it possible for organizations that want to

deploy or develop training platforms to objectively evaluate them is also introduced. This book is addressed first to cybersecurity education and training practitioners and professionals, both in the academia and industry, who will gain knowledge about how to organize and conduct meaningful and effective cybersecurity training activities. In addition, researchers and postgraduate students will gain insights into the state-of-the-art research in the field of cybersecurity training so that they can broaden their research area and find new research topics.
