1. Record Nr. UNINA9910847580503321

Autore	Huang Ken
Titolo	Generative AI Security : Theories and Practices / / edited by Ken Huang, Yang Wang, Ben Goertzel, Yale Li, Sean Wright, Jyoti Ponnapalli
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031542527 3031542525
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (367 pages)
Collana	Future of Business and Finance, , 2662-2475
Altri autori (Persone)	WangYang GoertzelBen LiYale WrightSean PonnapalliJyoti
Disciplina	005.8
Soggetti	Business information services Financial risk management Data protection Artificial intelligence Information technology - Moral and ethical aspects IT in Business Risk Management Data and Information Security Artificial Intelligence Information Ethics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Foundations of Generative AI -- Navigating the GenAI Security -- AI Regulations -- Build Your Security Program for GenAI -- GenAI Data Security -- GenAI Model Security -- GenAI Application Level Security -- From LLMOps to DevSecOps for GenAI -- Utilizing Prompt Engineering to Operationalize Cyber Security -- Use GenAI Tools to Boost Your Security Posture.
Sommario/riassunto	This book explores the revolutionary intersection of Generative AI

(GenAI) and cybersecurity. It presents a comprehensive guide that intertwines theories and practices, aiming to equip cybersecurity professionals, CISOs, AI researchers, developers, architects and college students with an understanding of GenAI's profound impacts on cybersecurity. The scope of the book ranges from the foundations of GenAI, including underlying principles, advanced architectures, and cutting-edge research, to specific aspects of GenAI security such as data security, model security, application-level security, and the emerging fields of LLMOps and DevSecOps. It explores AI regulations around the globe, ethical considerations, the threat landscape, and privacy preservation. Further, it assesses the transformative potential of GenAI in reshaping the cybersecurity landscape, the ethical implications of using advanced models, and the innovative strategies required to secure GenAI applications. Lastly, the book presents an in-depth analysis of the security challenges and potential solutions specific to GenAI, and a forward-looking view of how it can redefine cybersecurity practices. By addressing these topics, it provides answers to questions on how to secure GenAI applications, as well as vital support with understanding and navigating the complex and ever-evolving regulatory environments, and how to build a resilient GenAI security program. The book offers actionable insights and hands-on resources for anyone engaged in the rapidly evolving world of GenAI and cybersecurity.