1. Record Nr. UNINA9911019818803321

Autore	Finney George
Titolo	Rise of the Machines : A Project Zero Trust Story
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2025 ©2025
ISBN	1-394-30372-6 1-394-35251-4
Edizione	[1st ed.]
Descrizione fisica	1 online resource (195 pages)
Disciplina	005.8
Soggetti	Computer security Artificial intelligence - Security measures Computer networks - Security measures Machine learning - Security measures Business enterprises - Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Foreword -- About the Authors -- Acknowledgments -- Introduction -- Chapter 1: AI-pocalypse Now -- Chapter 2: No Artificial Trusts Added -- Chapter 3: Generative AI -- Chapter 4: Arch-AI-tecting Controls -- Chapter 5: Trusty AI Sidekick -- Chapter 6: Smooth AI-operator -- Chapter 7: The Most Important Part of Zero Trust: People -- Chapter 8: AI-dentity Theft -- Chapter 9: Algorithms and Adversaries -- Chapter 10: The End of Trust -- Appendix A The Cast of Characters -- Appendix B Tabletop Exercise: Master Scenario Events List -- Glossary -- Endnotes -- Index.
Sommario/riassunto	Expert guide to create Zero Trust digital environments in an AI-everywhere landscape Rise of the Machines: A Project Zero Trust Story is a continuation of the 2023 bestseller Project Zero Trust, picking up where the first book left off and addressing issues not covered in the first installment: artificial intelligence, mergers and acquisitions, antivirus, business continuity, and remote work. Artificial Intelligence is the dominant issue discussed in every chapter, providing a case-study-based approach to applying zero trust principles to all the various aspects of artificial intelligence, from MLOps, used by security teams,

to use of GPTs, chatbots, and adversarial AI. AI transforms technology by enabling unprecedented automation and decision-making, but securing it with a Zero Trust approach is essential because AI inherently relies on trusted data and systems, making it a target for manipulation. The book also includes discussion around regulatory issues and the alignment of regulation around Zero Trust practices. Written by George Finney, 2024 recipient of the Baldrige Foundation Leadership Award for Cybersecurity and recognized as one of the top 100 CISOs in the world in 2022, this book provides key insights on: Appling the four Principles of Zero Trust to AI: Focusing On Business Outcomes, Designing From The Inside Out, Determining Who Or What Needs Access, and Inspecting And Logging All Traffic Using the five steps of the Zero Trust Methodology to secure AI technologies: Defining Your Protect Surface, Mapping Transaction Flows, Architecting Your Environment, Creating Zero Trust Policies, and Monitoring and Maintaining Your Environment The evolution of Adversarial AI to scale attacks and how security operations teams can integrate into the Zero Trust strategy to use AI to accelerate defense Rise of the Machines: A Project Zero Trust Story is a timely, essential read for all IT professionals across industries, including network engineers, system administrators, and cloud architects.