1. Record Nr. UNINA9910917779503321

Autore	Wendt Donnie W
Titolo	The Cybersecurity Trinity : Artificial Intelligence, Automation, and Active Cyber Defense / / by Donnie W. Wendt
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2024
ISBN	9798868809477 9798868809460
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (410 pages)
Disciplina	005.8
Soggetti	Computer security Artificial intelligence - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Chapter 1: AI is Everywhere -- Chapter 2: Overview of AI and ML -- Chapter 3: AI for Defense -- Chapter 4: ML in an Adversarial Environment -- Chapter 5: Combatting AI Threats -- Chapter 6: The Need for Speed – The Driving Forces of Security Automation -- Chapter 7: The OODA Loop -- Chapter 8: Common SOAR Use Cases -- Chapter 9: Strategies for Success (and Failure) -- Chapter 10: Active Cyber Defense -- Chapter 11: The OODA Loop Revisited -- Chapter 12: Deception -- Chapter 13: The Cybersecurity Trinity.
Sommario/riassunto	This book explores three crucial topics for cybersecurity professionals: artificial intelligence (AI), automation, and active cyber defense (ACD). The Cybersecurity Trinity will provide cybersecurity professionals with the necessary background to improve their defenses by harnessing the combined power of these three concepts. The book is divided into four sections, one addressing each underlying concept and the final section discussing integrating them to harness their full potential. With the expected growth of AI and machine learning (ML), cybersecurity professionals must understand its core concepts to defend AI and ML-based systems. Also, most cybersecurity tools now incorporate AI and ML. However, many cybersecurity professionals lack a fundamental understanding of AI and ML. The book's first section aims to demystify AI and ML for cybersecurity practitioners by exploring how AI and ML

systems work, where they are vulnerable, and how to defend them. Next, we turn our attention to security automation. Human-centered cyber defense processes cannot keep pace with the threats targeting organizations. Security automation can help defenders drastically increase the speed of detection and response. This section will discuss core use cases that security teams can implement, including intelligence processing, incident triage, detection, and response. This section will end with strategies for a successful security automation implementation and strategies that can lead to failure. Accelerating the defense is but one side of the equation. Defenders can also implement ACD methods to disrupt and slow the attacker. Of course, ACD spans a broad spectrum, including some that could raise legal and ethical concerns. This section will explore some ACD methods and discuss their applicability, as well as the need to include business, legal, and ethical considerations when implementing them. Security teams often treat AI, automation, and ACD as disparate solutions, addressing specific problems. However, there is much overlap, and security teams must develop a cohesive approach to realize the full potential. The last section combines these three concepts to form a comprehensive strategy. The resulting strategy will have AI as the foundation, incorporating automation to speed up defense and ACD to disrupt the attacker. What You Will Learn: Understand the many uses of AI and ML and the concepts underpinning these technologies. Learn how to protect AI and ML systems by recognizing the vulnerabilities throughout their lifecycle. Integrate AI and ML-based systems to enhance cybersecurity. Develop security automation processes to enhance situation awareness, speed the time to respond, and increase the bandwidth of the limited security operations staff. Develop an ACD strategy to slow the attackers while minimizing legal and ethical concerns. Design a comprehensive strategy with AI as the foundation, incorporating automation to speed up defense and ACD to disrupt the attacker.