1.

Record Nr.	UNISA996464397603316
Autore	Badhwar Raj
Titolo	The CISO'S next frontier : AI, post-quantum cryptography and advanced security paradigms / / Raj Badhwar
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-75354-9
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (XLIII, 387 p. 14 illus., 11 illus. in color.)
Disciplina	005.8
Soggetti	Computer security Computer networks - Security measures Quantum computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Are you ready for Quantum computing? -- The need for post-quantum cryptography -- Quantum Encryption is not a Paradox -- AI Code of Ethics for Cybersecurity -- The Case of AI/ML in Cybersecurity -- Security for Work-From-Home Technologies -- Secure video conferencing and online collaboration -- If you must work from home, do it securely! -- Security Controls for Remote Access Technologies -- Specialty Malware and backdoors for VDI -- The Future State of Data Security -- Cybersecurity enabled by Zero Trust -- Advanced Active Directory attacks and Prevention -- Cyber Deception Systems -- Hypervisor Introspection -- Bitcoin is a decade old, and so are the threats to the various blockchain ecosystems -- The advanced malware prevention playbook -- The 768K Precipice -- MAC Address Randomization to limit user/device tracking -- Transport Layer Security 1.3 -- The use of ESNI with TLS 1.3, is it a boon to privacy? Or does it raise security concerns -- Using FQDN vs IP addresses in FW rules and app configs -- Network Time Protocol (NTP) Security -- Domain Name System (DNS) Security -- Next Gen Wi-Fi and Security -- The next frontier for CA/Certificate security - DANE and Certificate Transparency -- Man-in-the-middle Attack Prevention -- Distributed Denial of Service (DDoS) Prevention -- Intro to API Security – Issues and Some Solutions! -- Windows subsystem for Linux - security risk and

mitigation -- Common sense security measures for voice activated assistant devices -- The case for code signing and dynamic white-listing -- Biometrics - Commentary on data breach notification, threats, and data security -- Security requirements for RPA Bots -- Polymorphic and Metamorphic Malware -- Introduction to Cloud Monitoring Security Controls -- Cloud Monitoring Security Controls for AWS -- Cloud Monitoring Security Controls for Azure -- Cloud Policy Enforcement Point -- Dynamic measurement of cyber risk -- OEM and third-party sourced application and services risk -- Commentary on Insider Threat -- Simplified approach to calculate the probability of a cyber event -- Privacy concerns from publicly available meta-data -- Dark Web & Dark Net -- Risk-Based Vulnerability Management.

Sommario/riassunto

This book provides an advanced understanding of cyber threats as well as the risks companies are facing. It includes a detailed analysis of many technologies and approaches important to decreasing, mitigating or remediating those threats and risks. Cyber security technologies discussed in this book are futuristic and current. Advanced security topics such as secure remote work, data security, network security, application and device security, cloud security, and cyber risk and privacy are presented in this book. At the end of every chapter, an evaluation of the topic from a CISO's perspective is provided. This book also addresses quantum computing, artificial intelligence and machine learning for cyber security The opening chapters describe the power and danger of quantum computing, proposing two solutions for protection from probable quantum computer attacks: the tactical enhancement of existing algorithms to make them quantum-resistant, and the strategic implementation of quantum-safe algorithms and cryptosystems. The following chapters make the case for using supervised and unsupervised AI/ML to develop predictive, prescriptive, cognitive and auto-reactive threat detection, mitigation, and remediation capabilities against advanced attacks perpetrated by sophisticated threat actors, APT and polymorphic/metamorphic malware. CISOs must be concerned about current on-going sophisticated cyber-attacks, and can address them with advanced security measures. The latter half of this book discusses some current sophisticated cyber-attacks and available protective measures enabled by the advancement of cybersecurity capabilities in various IT domains. Chapters 6-10 discuss secure remote work; chapters 11-17, advanced data security paradigms; chapters 18-28, Network Security; chapters 29-35, application and device security; chapters 36-39, Cloud security; and chapters 40-46 organizational cyber risk measurement and event probability. Security and IT engineers, administrators and developers, CIOs, CTOs, CISOs, and CFOs will want to purchase this book. Risk personnel, CROs, IT and Security Auditors as well as security researchers and journalists will also find this useful.