1.	Record Nr.	UNINA9911047705003321
	Autore	Udayakumar Puthiyavan
	Titolo	Design and Deploy Microsoft Azure Sentinel for IoMT : Enhance IoMT Cybersecurity Operations with Intelligent Analytics / / by Puthiyavan Udayakumar, Dr. R Anandan
	Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2025
	ISBN	979-88-6882-040-3
	Edizione	[1st ed. 2025.]
	Descrizione fisica	1 online resource (337 pages)
	Collana	Professional and Applied Computing Series
	Disciplina	004.67/8
	Soggetti	Internet of things - Security measures Medical instruments and apparatus - Technological innovations - Security measures Microsoft Azure (Computing platform)
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Chapter 1: Get Started with Microsoft Sentinel and IoMT -- Chapter 2: Architecting and Deploying Microsoft Sentinel -- Chapter 3: Engineering Microsoft Sentinel for Security Operations -- Chapter 4: Threat Detection, Investigation, and Response.
	Sommario/riassunto	Microsoft Sentinel for Internet of Medical Things (IoMT) provides advanced threat detection, investigation, and automated response for connected medical devices, guaranteeing real-time protection in healthcare environments. The book guides you to deploy, and optimize Microsoft Sentinel specifically for IoMT environments, guaranteeing the protection of critical medical systems and patient data. The book starts with introducing the fundamental concepts of Sentinel, its role in securing IoMT, and the latest advancements in healthcare cybersecurity. Architecting and Deploying Microsoft Sentinel focuses on designing a Sentinel workspace tailored for IoMT, integrating medical device logs, and applying Zero Trust principles to secure connected healthcare environments. Engineering Microsoft Sentinel for Security Operations explores how security engineers can configure analytics, automate threat response, and optimize Security Operations Center (SOC) workflows to mitigate IoMT-specific threats, such as ransomware attacks on medical devices or unauthorized access to patient records.

Finally, Threat Detection, Investigation, and Response provides practical techniques for security analysts, including crafting detection rules for IoMT anomalies, investigating incidents involving medical devices, and leveraging Kusto Query Language (KQL) to proactively hunt for threats in healthcare networks. By the end of this book, you will be equipped to design, implement, and operate a comprehensive security framework for IoMT environments using Microsoft Sentinel. What You Will Learn: Design and deploy a Microsoft Sentinel workspace tailored specifically for IoMT, including integrating medical device logs. Implementing Zero Trust security principles to safeguard connected healthcare systems. Gain practical skills in creating custom detection rules for IoMT devices, investigating security incidents involving medical systems Understanding compliance with key healthcare regulations (such as HIPAA, GDPR, and FDA).