1. Record Nr. UNINA9910795111403321

Autore	Kaustubh Dhondge
Titolo	Lifecycle IoT Security for Engineers
Pubbl/distr/stampa	Norwood : , : Artech House, , 2021 ©2021
ISBN	1-5231-4587-0 1-63081-804-6
Descrizione fisica	1 online resource (219 pages)
Disciplina	004.678
Soggetti	Internet of things - Security measures Internet of things - Industrial applications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	This comprehensive resource provides a thorough introduction to the security risks, attack vectors and vulnerabilities an Internet of things (IoT) product and its network can face at different phases of its lifecycle. The risks at each stage of the development and operations (DevOps) lifecycle of an IoT product are analyzed. Examples of recent, relevant security threats faced by the industry are discussed and why the security breach happened, how it was resolved, and what could have been done to avoid them will be explained. Readers will learn the best practices to secure their IoT products, and networks in a holistic way. IoT and the diverse and unique nature of IoT applications across the commercial and industrial landscape, are introduced, including the need for securing IoT. The lifecycle of IoT security, specifically the security implementations that need to be carried out at various stages in the operational process of an IoT service are presented, as well as the security requirements during the planning, security integration, operational, maintenance, and planned discontinuation phase of an IoT service. The vulnerabilities in IoT, the various attack vectors exploited by attackers, and preventive measures that can be undertaken to avoid these security attacks are also explored. Readers are acclimated with various steps that must be undertaken to prepare for IoT security

attacks, and techniques that can be employed to detect them. Key challenges involved with implementing appropriate levels of security in IoT due to heterogeneity, interoperability, human errors, and commercial factors are discussed, as well as the need for regulatory guidance for the IoT industry and highlights specific examples of regulations in leading markets across the globe.