1. Record Nr. UNINA9910770247303321

Autore	Sadovykh Andrey
Titolo	CyberSecurity in a DevOps Environment [[electronic resource]] : From Requirements to Monitoring / / edited by Andrey Sadovykh, Dragos Truscan, Wissam Mallouli, Ana Rosa Cavalli, Cristina Seceleanu, Alessandra Bagnato
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-42212-0
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (329 pages)
Altri autori (Persone)	TruscanDragos MallouliWissam CavalliAna Rosa SeceleanuCristina BagnatoAlessandra
Disciplina	005.10289
Soggetti	Software engineering Data protection Computer programs - Testing Cooperating objects (Computer systems) Software Engineering Data and Information Security Software Testing Cyber-Physical Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Part I: Security Requirements Engineering -- 1. A Taxonomy of Vulnerabilities, Attacks, and Security Solutions in Industrial PLCs -- 2. Natural Language Processing with Machine Learning for Security Requirements Analysis - Practical Approaches -- 3. Security Requirements Formalisation with RQCODE -- Part II: Prevention at Development Time -- 4. Vulnerability Detection and Response: Current Status and New Approaches -- 5. Metamorphic Testing for Verification and Fault Localization in Industrial Control Systems -- 6. Interactive Application Security Testing with Hybrid Fuzzing and Statistical

Estimators -- Part III: Protection at Operations -- 7. CTAM: a tool for Continuous Threat Analysis and Management -- 8. EARLY - a tool for real-time security attack detection -- 9. A Stream-Based Approach to Intrusion Detection -- 10. Towards Anomaly Detection using Explainable AI. .

Sommario/riassunto

This book provides an overview of software security analysis in a DevOps cycle including requirements formalisation, verification and continuous monitoring. It presents an overview of the latest techniques and tools that help engineers and developers verify the security requirements of large-scale industrial systems and explains novel methods that enable a faster feedback loop for verifying security-related activities, which rely on techniques such as automated testing, model checking, static analysis, runtime monitoring, and formal methods. The book consists of three parts, each covering a different aspect of security engineering in the DevOps context. The first part, "Security Requirements", explains how to specify and analyse security issues in a formal way. The second part, "Prevention at Development Time", offers a practical and industrial perspective on how to design, develop and verify secure applications. The third part, "Protection at Operations", eventually introduces tools for continuous monitoring of security events and incidents. Overall, it covers several advanced topics related to security verification, such as optimizing security verification activities, automatically creating verifiable specifications from security requirements and vulnerabilities, and using these security specifications to verify security properties against design specifications and generate artifacts such as tests or monitors that can be used later in the DevOps process. The book aims at computer engineers in general and does not require specific knowledge. In particular, it is intended for software architects, developers, testers, security professionals, and tool providers, who want to define, build, test, and verify secure applications, Web services, and industrial systems.