1.
Record Nr.	UNISA996472069303316
Autore	Koodziej Joanna
Titolo	Cybersecurity of digital service chains : challenges, methodologies, and tools / / editors, Joanna Koodziej, Matteo Repetto, Armend Duzha
Pubbl/distr/stampa	Cham, : Springer International Publishing AG, 2022
ISBN	3-031-04036-8
Descrizione fisica	1 online resource (xi, 257 pages) : illustrations (chiefly color)
Collana	Lecture notes in computer science ; v.13300
Altri autori (Persone)	RepettoMatteo DuzhaArmend
Soggetti	Business - Data processing - Security measures Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	A Reference Architecture for Management of Security Operations in Digital Service Chains Efficient flow monitoring in digital services Intelligent Transportation Systems models, challenges, security aspects NAD: Machine Learning based Component for Unknown Attack Detection in Network Traffic Detecting unknown attacks through system behavior analysis Signature-based detection of botnet DDoS attacks Automatic Attack Pattern Mining for Generating Actionable CTI Applying Alert Aggregation Blockchain-based task and information management in computational cloud systems
Sommario/riassunto	This open access book presents the main scientific results from the H2020 GUARD project. The GUARD project aims at filling the current technological gap between software management paradigms and cybersecurity models, the latter still lacking orchestration and agility to effectively address the dynamicity of the former. This book provides a comprehensive review of the main concepts, architectures, algorithms, and non-technical aspects developed during three years of investigation; the description of the Smart Mobility use case developed at the end of the project gives a practical example of how the GUARD platform and related technologies can be deployed in practical scenarios. We expect the book to be interesting for the broad group of researchers, engineers, and professionals daily experiencing the

inadequacy of outdated cybersecurity models for modern computing environments and cyber-physical systems.