1. Record Nr. UNISA996547960403316

| | |
|---|---|
| Titolo | Collaborative Approaches for Cyber Security in Cyber-Physical Systems [[electronic resource] /] / edited by Theo Dimitrakos, Javier Lopez, Fabio Martinelli |
| Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023 |
| ISBN | 3-031-16088-6 |
| Edizione | [1st ed. 2023.] |
| Descrizione fisica | 1 online resource (XII, 226 p. 65 illus., 48 illus. in color.) |
| Collana | Advanced Sciences and Technologies for Security Applications, , 2363-9466 |
| Disciplina | 005.8 |
| Soggetti | Data protection<br>Computer crimes<br>Business information services<br>Security systems<br>Data and Information Security<br>Cybercrime<br>IT in Business<br>Security Science and Technology |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di contenuto | 1. Collaborative and confidential architectures for information sharing and analytics -- 2. Secure Interconnection of large-scale CPS-based frameworks and middleware -- 3. Virtualized security-awareness systems and digital twins -- 4. Empirical evaluation of system vulnerabilities -- 5. Collaborative physical and cyber defense requirements -- 6. Heterogeneous data centric security policies specification and enforcement -- 7. Big data for anomaly and advanced threats detection -- 8. Collaborative identification and ranking of malware -- 9. Visual analytics techniques for cyber security -- 10. Collaborative mitigation methodologies against advanced and persistent attacks. |
| Sommario/riassunto | This book describes cyber-security issues underpinning several cyber-physical systems and several application domains, proposing a |

common perspective able to collect similarities as well as depict divergences and specific solution methods. Special attention is given to those approaches and technologies that unleash the power of collaboration among stakeholders, in a field based often developed in isolation and segregation of information. Given the pervasively growing dependency of society on IT technology, and the corresponding proliferation of cyber-threats, there is both an imperative need and opportunity to develop a coherent set of techniques to cope with the changing nature of the upcoming cyber-security challenges. These include evolving threats and new technological means to exploit vulnerabilities of cyber-physical systems that have direct socio-technical, societal and economic consequences for Europe and the world. We witness cyber-attacks on large scale infrastructures for energy, transport, healthcare systems and smart systems. The interplay between security and safety issues is now paramount and will be even more relevant in the future. The book collects contributions from a number of scientists in Europe and presents the results of several European Projects, as NeCS, SPARTA, E-CORRIDOR and C3ISP. It will be of value to industrial researchers, practitioners and engineers developing cyber-physical solutions, as well as academics and students in cyber-security, ICT, and smart technologies in general. .