1. Record Nr. UNINA9910299269203321

Autore	Nunes Eric
Titolo	Artificial Intelligence Tools for Cyber Attribution / / by Eric Nunes, Paulo Shakarian, Gerardo I. Simari, Andrew Ruef
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-319-73788-0
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (97 pages) : illustrations
Collana	SpringerBriefs in Computer Science, , 2191-5768
Disciplina	006.3
Soggetti	Artificial intelligence Data protection Artificial Intelligence Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references at the end of each chapters.
Sommario/riassunto	This SpringerBrief discusses how to develop intelligent systems for cyber attribution regarding cyber-attacks. Specifically, the authors review the multiple facets of the cyber attribution problem that make it difficult for “out-of-the-box” artificial intelligence and machine learning techniques to handle. Attributing a cyber-operation through the use of multiple pieces of technical evidence (i.e., malware reverse-engineering and source tracking) and conventional intelligence sources (i.e., human or signals intelligence) is a difficult problem not only due to the effort required to obtain evidence, but the ease with which an adversary can plant false evidence. This SpringerBrief not only lays out the theoretical foundations for how to handle the unique aspects of cyber attribution – and how to update models used for this purpose – but it also describes a series of empirical results, as well as compares results of specially-designed frameworks for cyber attribution to standard machine learning approaches. Cyber attribution is not only a challenging problem, but there are also problems in performing such research, particularly in obtaining relevant data. This SpringerBrief describes how to use capture-the-flag for such research, and describes

issues from organizing such data to running your own capture-the-flag specifically designed for cyber attribution. Datasets and software are also available on the companion website.