CyberRank: Knowledge Elicitation for Risk Assessment of Database Security

Title	CyberRank: Knowledge Elicitation for Risk Assessment of Database Security
Publication Type	Conference Paper
Year of Publication	2016
Authors	Grushka - Cohen, Hagit, Sofer, Oded, Biller, Ofer, Shapira, Bracha, Rokach, Lior
Conference Name	Proceedings of the 25th ACM International on Conference on Information and Knowledge Management
Publisher	ACM
Conference Location	New York, NY, USA
ISBN Number	978-1-4503-4073-1
Keywords	cold start, cyber security, expert systems, Human Behavior, human factors, preference elicitation, privacy, pubcrawl, ranking, risk assessment, Scalability, semi supervised
Abstract	Security systems for databases produce numerous alerts about anomalous activities and policy rule violations. Prioritizing these alerts will help security personnel focus their efforts on the most urgent alerts. Currently, this is done manually by security experts that rank the alerts or define static risk scoring rules. Existing solutions are expensive, consume valuable expert time, and do not dynamically adapt to changes in policy. Adopting a learning approach for ranking alerts is complex due to the efforts required by security experts to initially train such a model. The more features used, the more accurate the model is likely to be, but this will require the collection of a greater amount of user feedback and prolong the calibration process. In this paper, we propose CyberRank, a novel algorithm for automatic preference elicitation that is effective for situations with limited experts' time and outperforms other algorithms for initial training of the system. We generate synthetic examples and annotate them using a model produced by Analytic Hierarchical Processing (AHP) to bootstrap a preference learning algorithm. We evaluate different approaches with a new dataset of expert ranked pairs of database transactions, in terms of their risk to the organization. We evaluated using manual risk assessments of transaction pairs, CyberRank outperforms all other methods for cold start scenario with error reduction of 20%.
URL	http://doi.acm.org/10.1145/2983323.2983896
DOI	10.1145/2983323.2983896

Citation Key grushka_-_cohen_cyberrank:_2016

cyber security risk assessment pubcrawl Human behavior privacy Scalability cold start preference elicitation ranking semi supervised expert systems Human Factors