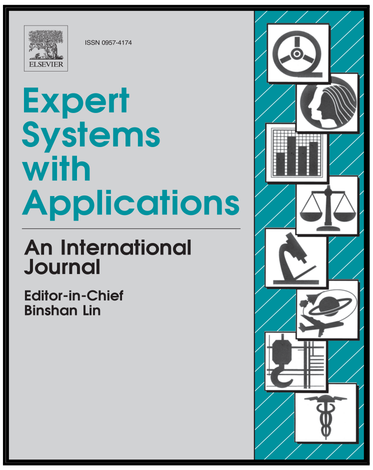
Accepted Manuscript



Eliciting and utilising knowledge for security event log analysis: an association rule mining and automated planning approach

Saad Khan, Simon Parkinson

PII: S0957-4174(18)30422-6
DOI: 10.1016/j.eswa.2018.07.006
Reference: ESWA 12055

To appear in: *Expert Systems With Applications*

Received date: 22 January 2018
Revised date: 4 June 2018
Accepted date: 2 July 2018

Please cite this article as: Saad Khan, Simon Parkinson, Eliciting and utilising knowledge for security event log analysis: an association rule mining and automated planning approach, *Expert Systems With Applications* (2018), doi: 10.1016/j.eswa.2018.07.006

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Highlights

- Generating object-based models of Microsoft Windows event logs for analysis
- Using temporal-association rule mining to generate chains of related events
- Encoding chains of events into PDDL domain models for automated planning
- Extracting action plan traces for vulnerable machines using the expert knowledge
- Provisioning expert knowledge to non-experts with reasonable performance and accuracy

ACCEPTED MANUSCRIPT

Download English Version:

https://daneshyari.com/en/article/6854699

Download Persian Version:

https://daneshyari.com/article/6854699

Daneshyari.com