Title: A comparative analysis of incident reporting formats

Author: Florian Menges, Günther Pernul

PII: S0167-4048(17)30225-0
DOI: https://doi.org/10.1016/j.cose.2017.10.009
Reference: COSE 1221

To appear in: *Computers & Security*

Received date: 21-4-2017
Revised date: 11-10-2017
Accepted date: 27-10-2017

Please cite this article as: Florian Menges, Günther Pernul, A comparative analysis of incident reporting formats, *Computers & Security* (2017), https://doi.org/10.1016/j.cose.2017.10.009.

Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Economics and Finance 00 (2012) 000–000

Procedia
Economics and Finance

www.elsevier.com/locate/procedia

A Comparative Analysis of Incident Reporting Formats

Florian Menges and Günther Pernul

University of Regensburg, Department of Information Systems
Universitätsstraße 31, 93053 Regensburg, Germany

Abstract

Over the past few years, the number of attacks against IT systems and the resulting incidents has steadily increased. To protect against these attacks, joint approaches, which include the sharing of incident information, are increasingly gaining in importance. Several incident reporting formats build the basis for information sharing. However, it is often not clear how to design the underlying processes and which formats would fit the specific use cases. To close this gap, have introduced an incident reporting process model and the generic model UPSIDE for basic incident reporting requirements. Subsequently, we have identified state-of-the-art incident reporting formats and used the introduced models to conduct a comparative analysis of these formats. This analysis shows the strengths and weaknesses of the evaluated formats and identifies the use cases for which they are suitable.

Keywords: Incident reporting, incident management, incident response, reporting formats, STIX, IODEF, IODEF-SCI, VERIS, X-ARF

Günther Pernul received both the diploma degree and the doctorate degree (with honors) from the University of Vienna, Austria. Currently he is full professor at the Department of Information Systems at the University of Regensburg, Germany. Prior he held positions with the University of Duisburg-Essen, Germany and with University of Vienna, Austria, and visiting positions the University of Florida and the College of Computing at the Georgia Institute of Technology, Atlanta. His research interests are manifold, covering data and information security aspects, data protection and privacy, data analytics, and advanced data centric applications.

Florian Menges received both the Bachelor of Science and Master of Science degree from the University of Regensburg, Germany. Currently he is research assistant at the Department of Information Systems at the University of Regensburg, Germany. His research interests include threat intelligence with a focus on sharing and reporting intelligence data, storage strategies for intelligence data as well as anonymization techniques and incentivizing the sharing and reporting of incident data.