

Eliminating noise from intrusion detection systems

Gerhard Eschelbeck ^a and Michael Krieger ^b

^a Qualys, USA

^b University of Linz, Austria

Available online 31 December 2003.

Abstract

Effective noise reduction for intrusion detection systems (IDS) is a continuous area of research. One of the techniques for eliminating unqualified IDS alerts is to correlate them with environmental intelligence about the network and systems. This article provides an overview of correlation requirements with a proposed architecture and solution for the correlation and classification of IDS alerts in real time. The implementation of the QuIDScore correlation engine was validated on a real-world network and demonstrated a significant reduction of false alerts.