Information Security for South Africa (ISSA) Conference, Johannesburg, South Africa, 14 - 16 August 2013

Classification of Security Operation Centers

Pierre Jacobs, Alapan Arnab, Barry Irwin
Department of Computer Science Rhodes University Grahamstown, South Africa
pjacobs@csir.co.za, alapan@gmail.com, b.irwin@ru.ac.za

Abstract

Security Operation Centers (SOCs) are a necessary service for organisations that want to address compliance and threat management. While there are frameworks in existence that addresses the technology aspects of these services, a holistic framework addressing processes, staffing and technology currently do not exist. Additionally, it would be useful for organizations and constituents considering building, buying or selling these services to measure the effectiveness and maturity of the provided services. In this paper, we propose a classification and rating scheme for SOC services, evaluating both the capabilities and the maturity of the services offered.