Frequently, Security Monitoring is equated with network intrusion detection. However, Security Monitoring has a much broader scope. It also comprises detection of insider attacks. Since the Enron bankruptcy, monitoring of privileged access to financial data has become a legal requirement stipulated for example in the Sarbanes-Oxley Act (SOX 404). Monitoring of privileged access requires evaluation of its necessity, permission, and correctness. As a result, detection of privileged access is not sufficient and must be reviewed in its business context. Data from various sources combined with business process contexts establish a sound basis for the assessment of a privileged access. Usually, the required data is spread over different data sources within an organization offering heterogeneous interfaces of any kind. Security administrators use multiple applications and data interfaces which result in a time-consuming and error prone process. Security Monitoring is, on the contrary, all about attack detection and prevention in a timely manner.

This paper introduces the concept of service-oriented context determination, which efficiently describes relationships between information entities originating from various applications and being stored in multiple data sources. Exploiting the architectural paradigm of service-oriented architecture (SOA), the concept establishes an integrated and task-oriented view of complex relationships and supports immediate reactions on suspicious events in the IT infrastructure.