



Contribution ID: 121

Type: oral

Information Management: Enhancing Information Discovery and Information Availability

Friday, 24 October 2014 12:00 (20 minutes)

IBM Security Intelligence with Analytics of massive data provides exceptional threat and risk detection, combining deep security expertise with analytical insights on a massive scale. For forward-leaning organizations seeking advanced insight into security risks, the IBM solution –Security Intelligence Platform for massive data –provides a comprehensive, integrated approach that combines real-time correlation for continuous insight, custom analytics across massive structured and unstructured data, and forensic capabilities for irrefutable evidence. The combination can help you address advanced persistent threats, fraud and insider threats.

The IBM solution is designed to widening the scope and scale of investigation, enabling analyzes of any kind of data in any format –such as DNS transactions or full packet capture data to find malicious activity hidden deep in the masses of an organization’s data.

IBM Watson Explorer provides a unified view displaying all of security relevant information in a portal like UI.

The information analytics system is built around AQL (Annotated query language), a declarative rule language with a familiar SQL-like syntax.

AQL supports the paradigm describing data for data with an optional data governance catalog for massive volumes of data supporting individual views in addition to the pre-defined Document view that holds the textual and label content.

An underlying Role-Based Access Control that data protection rules are strictly enforced within the whole architecture. Security at the document, sub-document and record level is built into Watson Explorer. When Watson Explorer security is implemented, users cannot see information that they would be prohibited from seeing if they were directly logged into the target system.

Country or International Organization

IBM Austria

Primary author: NIMFUEHR, Wolfgang (IBM)

Presenter: NIMFUEHR, Wolfgang (IBM)

Session Classification: Promoting the Interface Between Nuclear Safety, Security and Safeguards