Visualization of Workflow for Security Analytics

Graphics-Visualization-Computing Lab
International Institute of Information Technology, Bangalore

January 2014

Over the past few years, the security industry is seeing a transition from rule-based systems to leveraging advanced data analytics techniques (including machine learning) as the primary means of identifying security incidents. There is ongoing work to identify the right analytics algorithms and techniques which can be applied over scenarios, such as, different combinations of security data to satisfy different security intrusion, data ex-filtration detection, etc.

Given the composable and customizable nature of data analytics based security systems, this research proposal is based on the need for visualization in enabling building systems with data analytics components. Effective and intuitive visualization of security analytics enables the enterprise security incident response teams to consume the security analytics results for exploration and summarization, and additionally to make better informed decisions with regard to the correctness and criticality of the various components.