Insider Threats: A Case Study in Data Science

Insider threats present one of the greatest challenges in the cyber security community today. As evidenced by the recent headlines, an organization needs to be aware of threats existing within its own ranks. Either through neglect or intentional actions, a person can cause significant damage in theft, destruction, or espionage of critical information. Unlike red teaming or penetration exercises, catching insiders commonly boils down to an exercise in data science to sift through the volumes of log files. When working at a large organization, these datasets become too unwieldy to tackle through normal analytical methods. At FedCentric Technologies, we have address this problem by leveraging scale-up SGI UV platforms to perform rapid analysis on the problems, and identify/rank potential threats within minutes. In our presentation, we will discuss our research on insider threats, the technologies we employ, and why cyber security experts care about data science.