Data-Driven Analytics for Cyber-Threat Intelligence and Information Sharing

Date: April 13, 2017

Time: 11:30 Registration | 12:00 - 1:00 PM Lunch | 1:00 PM –3:00 PM Presentation
Networking event following the presentation

Location: Top Golf | 10611 Nall Avenue | Overland Park, Kansas 66207

CPE's: 2 Credits
*Please note actual CPE hours granted are dependent upon duration of speaker's presentation and may differ from advertised number of CPE hours.

Price: $35 members | $50 guests | $5 Students

Menu: Adobe Marinated Steak Fajitas, Char-Grilled Chicken Fajitas, Cilantro Savory Rice, and Chipotle Braised Black Beans
Please denote any dietary restrictions when registering and accommodations will be made.

Note: **Registration closes at 5 pm April 6, 2017.**

Presentation Overview:
There has been growing interest in implementing a proactive line of defense by understanding the attackers' intentions and capabilities and dynamically enforcing security perimeters through threat-impact-analysis based upon real-time cyber threat intelligence sharing (CTI). There are several community-driven efforts towards developing standardized languages to define cyber threats and document their instances reported at collaborating nodes. On-line threat repositories contain a wealth of attack information with public sources such as Hail-a-TAXII containing more than 1M threat indicators. However effectively utilizing these to make cyber defense decisions is tedious because of the sheer volume, diversity and textual nature of the data. In this talk we will examine some of the challenges to sharing, in light of the current CTI languages, repositories and frameworks in place. Furthermore the talk will discuss recent technological advances that allow machines to potentially perform analytics of CTI data, for its more effective utilization in sense-making and cyber defense decision-making in an organization.

Speaker Summary:
Zahid Anwar received his Ph.D. and M.S. degrees in Computer Sciences in 2008 and 2005 respectively from the University of Illinois at Urbana-Champaign. Zahid has worked as a software engineer and researcher at IBM, Intel, Motorola, NCSA, xFlow Research and CERN on projects related to information security and data analytics. Zahid has academic experience working as a post-doctorate fellow at Concordia University, Canada and as a faculty member at the University of North Carolina at Charlotte. Presently, he is an Assistant Professor at Fontbonne University, St. Louis.

Networking Event:
Join us for networking, golf, and beverages following the presentation.