Rich Voninski

Splunk, Inc.

Threat Hunting with Splunk

Abstract:

In this presentation we will talk about cyber threat hunting and the steps and data sources required in order to find cyber attacks. We will talk about different tools available with Splunk to help with analyzing security threats and also show a few examples of common threats and how to utilize Splunk to find and analyze these events.

Biography:

Rich has a diverse IT background and currently works for Splunk Software. He as a long history supporting enterprise users with IT Automation. Working for IBM as an Electrical Engineer and an Enterprise Systems Management Architect he pioneered IT Automation solutions for enterprise customers. He also has experience at PricewaterhouseCoopers as an Integration Consultant, and Microsoft as the MSDN Evangelist. He holds a Bachelor's degree in Electrical Engineering from Syracuse University.

Rich and his wife Veronica live in Aurora, CO and love to travel and take photographs in their spare time. He has visited all 50 states and is currently working towards visiting 50 countries (he's still stuck at 45). His other hobby is using IoT devices/software and solutions to automate his enterprise customers and his home.