**Session Title (75)**

Security Data Science: Detection & Defense Through Analysis & Visualization

**Short (400 chars) abstract**

We finally have the data we longed for but continue to struggle to make security-sense of it. This talk presents practical use cases based on real-world data and scenarios to introduce attendees to fundamental principles and practices in security data science, including data collection, munging, analysis and visualization.

**Quick (200 chars) abstract**

Learn core security data science tools and techniques for data collection, analysis and visualization with use cases based on real-world data.

**Session Detail (2500 chars)**

For years we've asked for "the data" and now we're swimming in a river of it, struggling to make security-sense of it all. Our systems, networks and applications are far too complex to rely on intuition alone to secure. This session will empower the security practitioner to embrace a data-driven approach to defending their organizations and detecting malicious behavior.

Using real-world data and practical hands-on use cases with data anyone can download, attendees will be introduced to the fundamental tools and techniques of security data science, including data collection, munging, analysis and visualization. Topics will include IP address analysis (details), spatial mapping and the significance of geo-location services, and applying machine learning to netflow data to pull out patterns. You will see how to go from understanding a problem, to formulating a practical research question, performing a thorough analysis and communicating and applying the results. Along the way, you'll also see how to go from distributed data to dynamic dashboards.

Whether you are eager to discover the power of data or are an ardent data science skeptic, there's something in this session for everyone.

**Submitter Comments (400 chars)**

The presenters of this talk will be releasing a book on security data science at RSA through Wiley press. The topics covered in the session will have parallels in the book that attendees can use to study the principles & techniques in more detail. Title is “Security Using Data Analysis, Visualization, and Dashboards” ISBN 1118793722 at http://amzn.to/12d0w1R