

TRACK: InfraGard Track / Cyber-crime, terrorism, and information warfare
SESSION #: ITCT#6
DATE: Tuesday April 20, 2010
TIME: 9:50-11:05am
SESSION TITLE: "Obtaining Actionable Data & Network Intelligence using Analytical Cubes"
SPEAKER(S): Kent Stern, MCSE+I, MCT, MCSD, MCDBA, MCITP, MCTP, CTT, CNA, CISSP – Managing Director, Lead Data Mining Architecture
ORGANIZATION: CodeCenters International

ABSTRACT: "Obtaining Actionable Data & Network Intelligence using Analytical Cubes"

The ability to take large volumes of seemingly unrelated network or case data and validating your network state, whether secure or compromised is a primary investigative method that must be used in today's data centric world. In this presentation, Mr. Stern will cover the fundamentals associated with creating a baseline of normal, abnormal and outlier data activity in an enterprise using analytical cubes. He will review data dimensionality and the process that is needed to manually bring unrelated data sources into a data cube for analysis, mining and obtain actionable intelligence. Case studies will be used to cover the concept of data dimensions and fact tables.

1. Enterprise packet and data analysis (large volumes of data and processing times (300 Million plus rows). Analyzing packet logs from one router or firewall is easy, but what if you have 50 routers and all packets from all routers must be analyzed over a 12 month period. Also, is real time notification possible with terabytes of data?
2. Analysis on large volumes of data that seems unrelated or has limited relationships (dimensionality). The horoscope scenario – How much information do I need to get a clear picture of the situation and how will I build the cube from that data.
3. What are the MDX and DMX languages and how can they be used to correlate data for intelligence gathering?
4. (As time permits) Correlating data from public records requests and law enforcement databases.

SPEAKER BIO(S): Kent Stern is the Managing Director and Lead Data Mining Architect at CodeCenters International, Inc. With over 23 years of focused database development and security experience, you will find him managing data intelligence projects for the global 100 and teaching data examination to corporations and Law enforcement worldwide. He has worked in diverse areas that range from oil exploration to health care and manufacturing to law enforcement. Additionally, he has written numerous training manuals such as "Producing Actionable Intelligence from Loosely Coupled Data", "Disaster Recovery for Exchange databases",

"Simplifying MDX Queries for Analytical Reporting" and "Building KPI's, Calculated Members and SSAS Cubes for Analysis".