

Evaluating Cyber Security Tools

Katherine Victoria Williams
 Saint Mary-of-the-Woods College
http://info.ornl.gov/sites/rams2012/k_williams/

Research Alliance in Math and Science
Computing and Computational Sciences Directorate

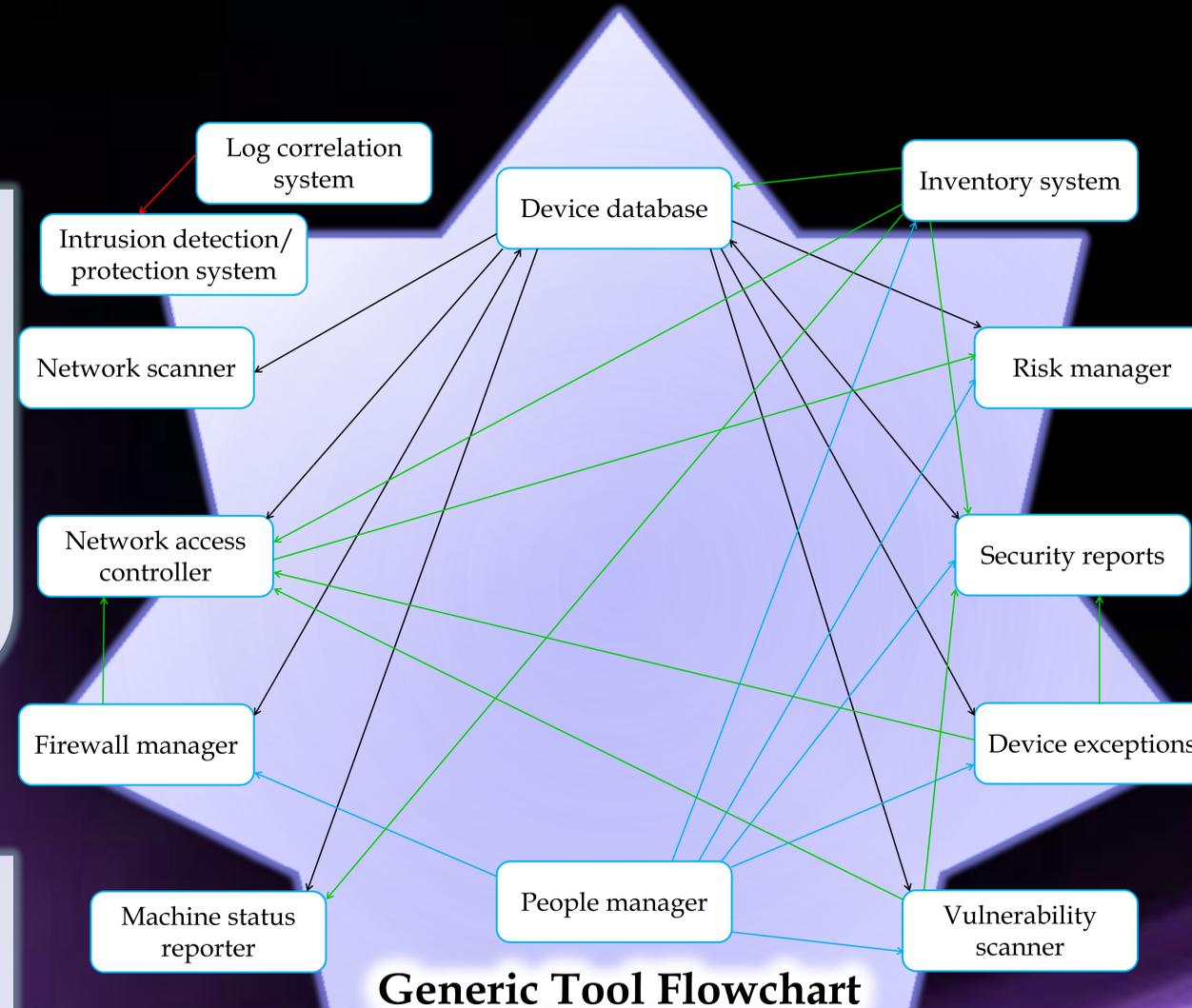
Mentors: Kevin Kerr and Tina Heath
 Information Technology Services Division
 Oak Ridge National Laboratory

Background

- Every security tool has its own data repository
- Must understand correlation between databases
- Know actual risk vs. industry-defined risk
- Can better categorize risks
- Allows more focus on actual critical risks
- Knowing data flow helps understand security
- Scoring vulnerabilities aids in determining risk to network

Methodology

- Discuss with tool experts regarding cyber security tool use
- Converse with tool administrators concerning managing security tool data
- Record all significant information
- Understand information being uncovered
- Identify problems and inconsistencies
- Organize information into useable format



Research Objectives

- Identify and list cyber security tools
- Conduct a literature survey on master data management
- Evaluate connections between current tools at Oak Ridge National Laboratory
- Create flow chart of security tool connections
- Determine specific data moving between tools
- Help create internal risk assessment score

Results

- Security tool flowchart revealing data connections
- Partially complete data exchange sheet
- Revelation of security tool gaps
- Risk index for internal systems (RIFIS) design and test begin
- Discover problem of no single source for information

Conclusions

- Large area of functionality
- Information not shared or viewed the same
- Identify vulnerabilities inside network to strengthen defenses
- Continuation of cyber security adaptability against new threats
- Current tools need evaluation for efficiency
- Evaluate current tools for better usage before purchase of new tools

