Proposing a Multi-touch Interface for Intrusion Detection Environments

Jeffrey Guenther, Fred Volk, and Mark Shaneck

The Problem

- Huge text-based network logs with more being created every second
- Context is difficult to acquire from detail level tools
- And only Jim knows what is really going on

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Analysts need tools which:

- Handle LARGE datasets
- Provide context
- Afford exploration
- Manage cognitive load

Essentially, the Fundamental Problem of Visual Analytics

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Current Visualizations

- Consensus on the need for more interactivity
  - Access to both detail and contextual information

- See Section 2.1 for a more detailed discussion

Getting to Know Analysts

- Need more than a CTA
- Activity Theory
  - provides a theoretical basis
  - need a multi-methods approach

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Applying Activity Theory Example

- Activities – keeping the network
- Actions – reviewing logs
- Operations – changing the configuration of a network sensor

A New Design Approach

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

A look at requirements:

- Monitoring
- Analysis
- Response
- Knowledge Management

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Monitoring

- Identify network state at a glance
- Use pre-attentive visual properties to control the amount required attention

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Analysis

- Goal: to develop understanding
- Multiple views at different levels of data abstraction

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Response

- Network management
- Parts of response:
  - Record the happening of an event
  - Affect network changes

Knowledge Management

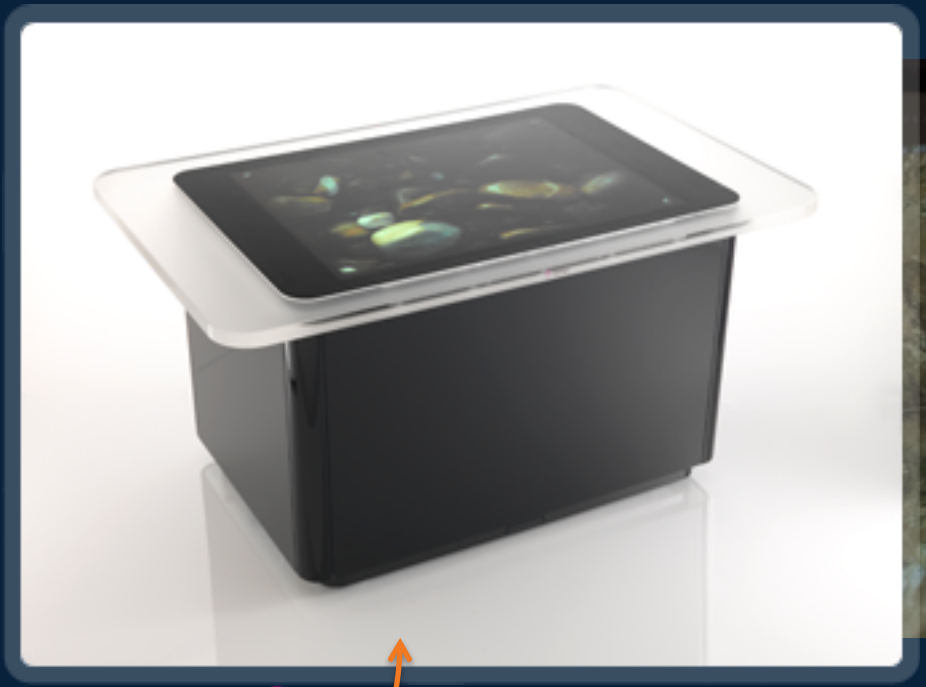
- Capture Jim's experience
- Provides a library of case studies for future training
- Must be a by product of using the tool, not an extra step

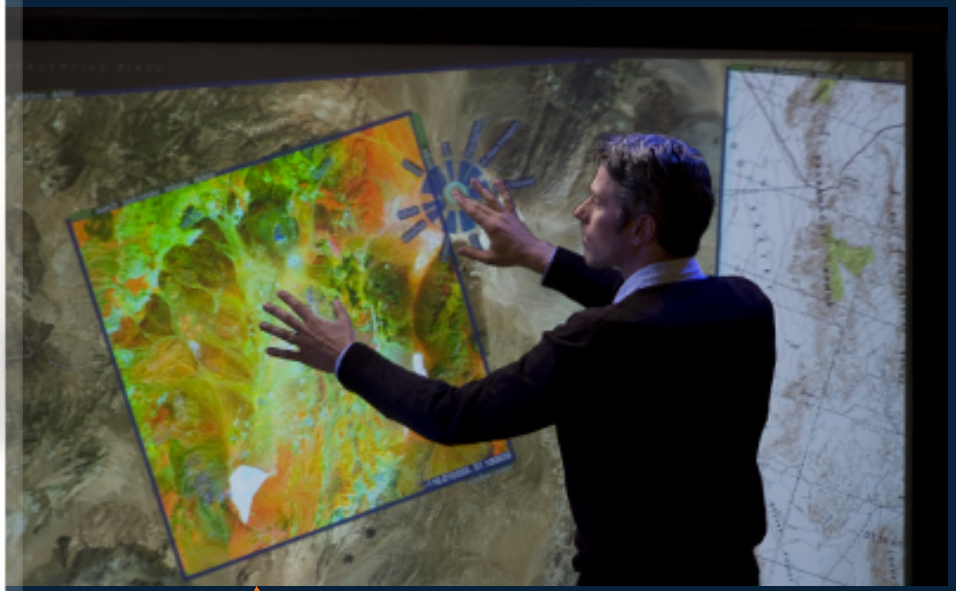
LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Our Design

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Multi-touch based network analytics tool





Microsoft Surface

PERCEPTIVE PIXEL

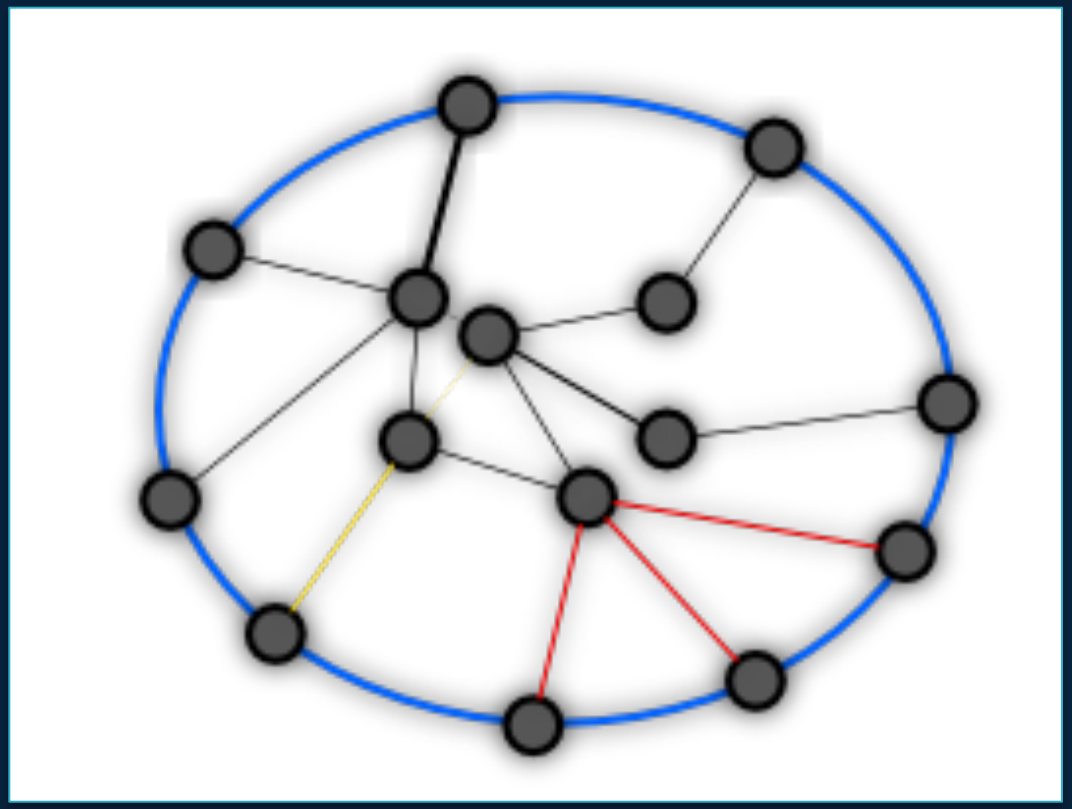
LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING AND COMPUTATIONAL SCIENCES

Affordances

- Physical (embodied) interaction with interface
- Gestures
- Faster interaction than with a mouse

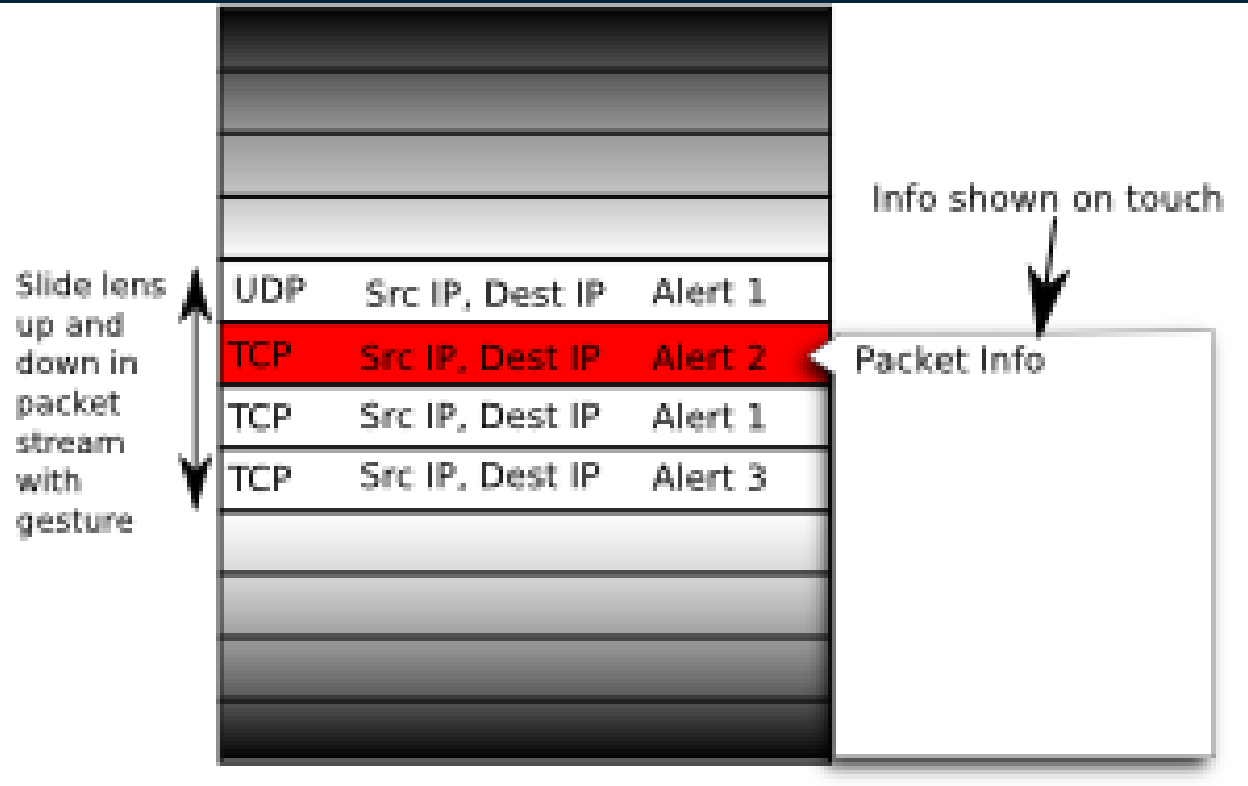
LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Zoomable, Spatial Exploration

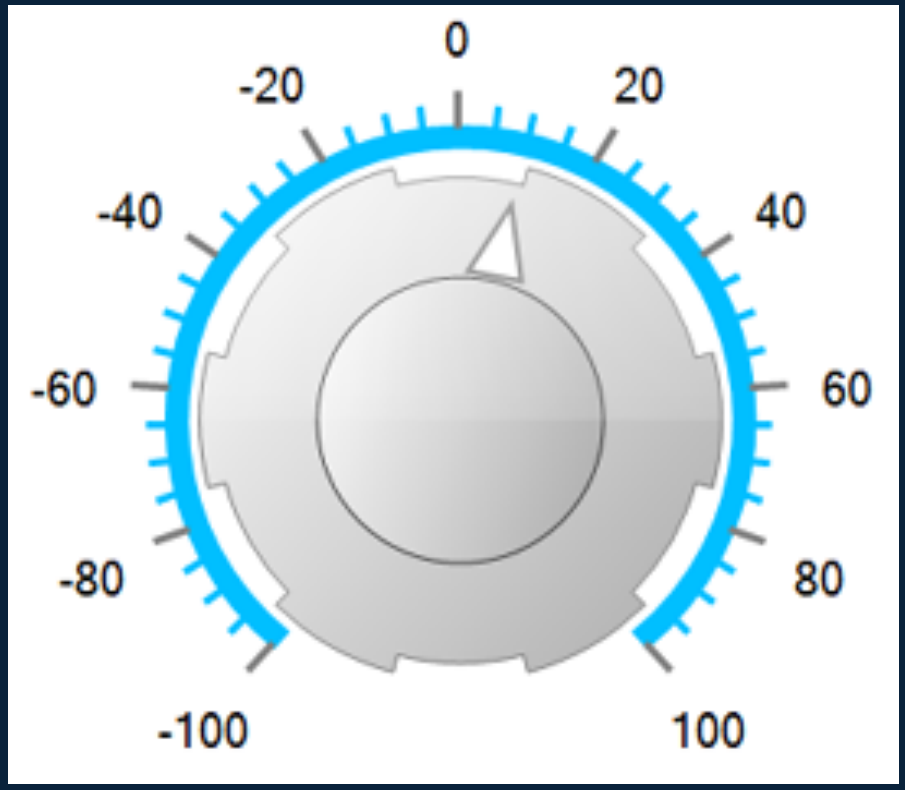


LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Packet Level



Time



devcomponents.com

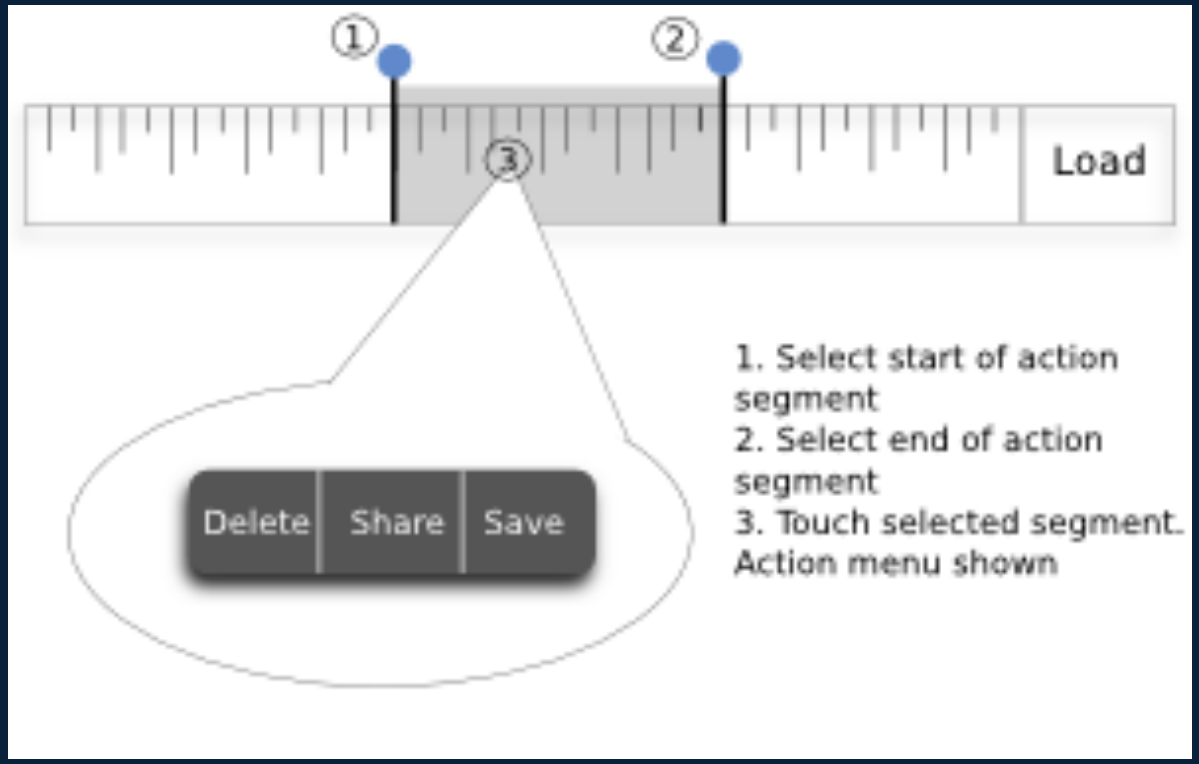
LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Using Metadata

- To learn context
- To describe interactions -> create knowledge base

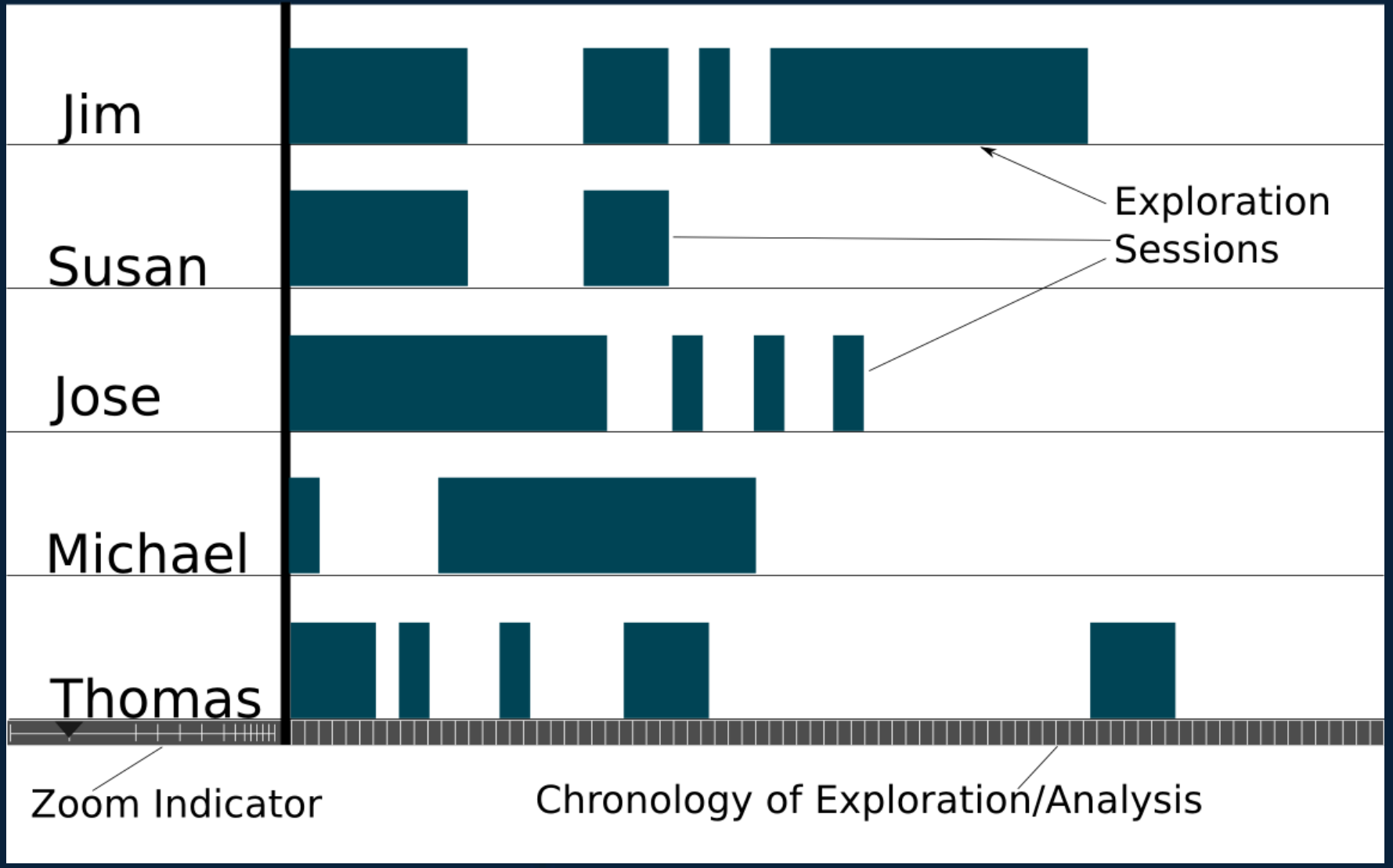
LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

ActionLine



LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Knowledge Tracks



User-refined Alert Correlation

- Make alert correlation interactive
  - Guided exploration of data

- Allow addition/removal of events from attack
- Correlation computation updated

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Wrapping Up

- Exposed the need for a multi-method research
- List of Requirements:
  - Monitoring
  - Analysis
  - Response
  - Knowledge Management
- Argued for a new mode of interaction

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES

Questions?

LIBERTY UNIVERSITY
SCHOOL OF ENGINEERING
AND COMPUTATIONAL SCIENCES