Exploring the Design Space for Cyber Alerts in Context

Michelle Dowling, Lyndsey Franklin, Mi Feng, Meg Pirrung, Robert Jaspar, Joseph Cottam, Leslie Blaha

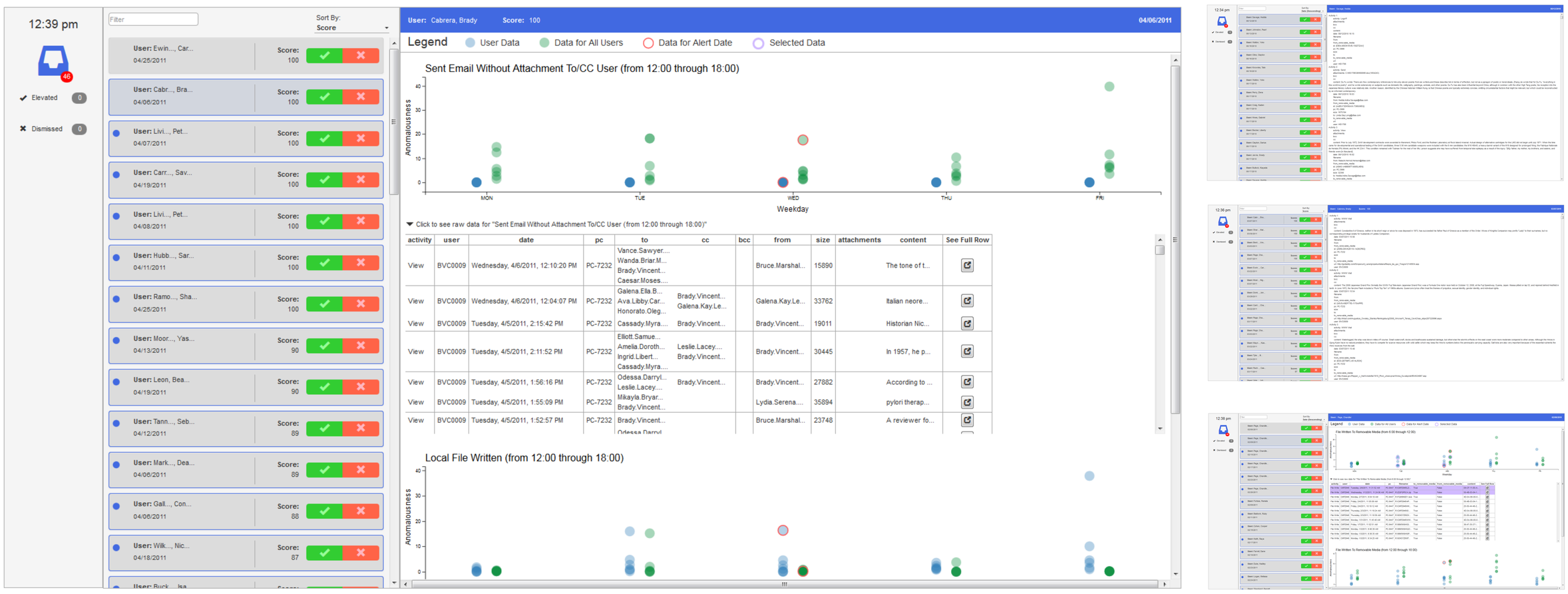
Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Overview

During knowledge elicitations with cyber analysts, we uncovered a need for tools that help analysts understand threat alerts in a context of baseline ``normal'' behaviors. We used an iterative design process to create a prototype alert management system with which we can explore the critical design space for effective baseline visualizations.

User Interface



Interface with automated machine support and interactive visualizations (left) and user study variations without machine support and text (right)

Alert Inbox

- Easy-to-grasp metaphor
- Supports constantly arriving alerts
- Maintains active to-do list and context
- Sorting and filtering to support prioritization of alerts
- 'Elevate' and 'Dismiss' actions available directly on alert
- Decisions can be reviewed in sub-folders as follow-up or verification

Automated Support

- Provides measure of anomalousness to support alert prioritization
- Normalized percentiles support comparison across users and days
- Feature space of detection algorithm used to structure visualization and explain alert score

Interactive Visualization

- Synchronized with alert selection
- User and larger network baselines featured
- Simple graphics with low learning curve
- Table to provide raw data with visualization
- Accommodates multiple data types
- Supports multiple resolutions of data

Putting it Together

The combined features of this prototype provide an effective baseline visualization that should:

- Highlight alert-triggering activity
- Provide activity history/context for the asset or user triggering an alert
- Provide activity history/context for other assets/users who should exhibit similar profiles
- Enable trace-back to the relevant raw data

Expert Feedback

Preliminary feedback sessions with expert cyber analysts using the above interface variations has provided a number of insights:

- Presence of anomaly scores result in elevation of high-scoring alerts without investigation
- Structure of visualization provided starting point for alert investigation
- Experts shifted from table to visualization with system use
- Network statistics requested by text-interface variation users looking for context and baselines
- Visualization supported dismissal of false-positives with minimal investigation
- Machine learning improved reported usability scores for both text and visualization conditions

U.S. DEPARTMENT OF ENERGY

www.pnnl.gov