

## Real-time Situational Understanding and Discovery of Cyber Attacks

### **Disclosure Number**

201303053

### **Technology Summary**

The invention relates to cyber security and more specifically to a tool that addresses the challenges of timely discovery and understanding of novel and sophisticated cyber attacks through the software integration of anomaly detection, maliciousness classification, real-time information visualization, and a context-aware learning feedback loop between users and algorithms. Situ, the Real-time Situational Understanding and Discovery of Cyber Attacks tool, allows security analysts and system administrators to acquire, maintain, and ensure situational understanding of their networked resources through continual integration of analysts' knowledge to train analytic models through modeling user interactions with both visualizations and data and automatically identifying the data points that labeling would best improve attack discovery. A novel architectural design of novel machine-learning techniques, novel visualizations, and novel user-interactivity components will enable analysts to find more complex attacks hidden in voluminous, high-dimensional, streaming data sets in cyber defense.

### **Inventor**

LASKA, JASON A

Computational Sciences & Engineering Div

### **Licensing Contact**

SIMS, DAVID L

UT-Battelle, LLC

Oak Ridge National Laboratory

Rm 124C, Bldg 4500N, MS: 6196

1 Bethel Valley Road

Oak Ridge, TN 37831

Office Phone: (865) 241-3808

E-mail: [SIMSDL@ORNL.GOV](mailto:SIMSDL@ORNL.GOV)

Note: The technology described above is an early stage opportunity. Licensing rights to this intellectual property may be limited or unavailable. Patent applications directed towards this invention may not have been filed with any patent office.