

Situ: Real-time Situational Understanding and Discovery of Cyber Attacks

Copyright Document Number

CR14-00022

Copyright Summary

Rapidly discovering novel and sophisticated cyber attacks and providing situation awareness to analysts are unsolved problems in cyber security. Researchers at ORNL have developed the Situ software platform for cyber attack discovery and situational understanding that focuses on probabilistic anomaly detection and streaming visualization. Situ scores events in real-time to define how typical an event is. This anomaly detection approach is based on unsupervised, probabilistic modeling of data at multiple scales. The system was designed to address several challenges including (1) scaling to very high volume, heterogeneous, streaming data and (2) minimizing the time from observation to discovery to understanding. The technology includes the real-time framework for pushing scored events into a web-based visualization. This software is a combination of Nodejs, JavaScript, and HTML. No special hardware is required.

Inventor

GOODALL, JOHN
Computational Sciences and Engineering Division

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

Note: The copyright described above is an early stage opportunity. Licensing rights to this intellectual property may be limited or unavailable.