OAK RIDGE NATIONAL LABORATORY

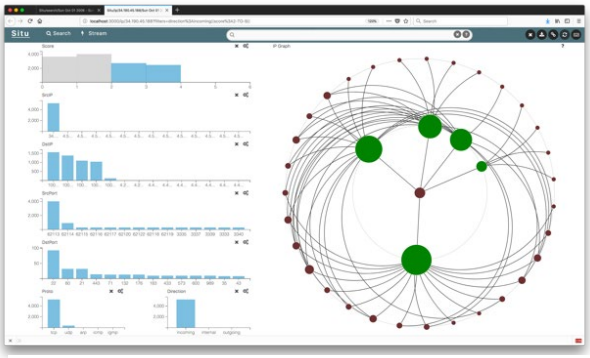
Situ

Discovering and explaining suspicious behavior for cybersecurity

Networked computing assets are regularly compromised, resulting in the loss of intellectual property, disclosure of state secrets, and financial damages in the billions. Sophisticated attack groups increasingly develop novel methods of penetrating networks, often undetectable by current signature-based systems.

While signature-based security systems can effectively detect known types of attacks, they often fail to detect novel or sophisticated attacks.

Situ helps network operators discover and understand suspicious events that would otherwise go undetected.



Situ provides a scalable, real-time platform for discovering and explaining suspicious behavior that current technologies cannot detect. Image credit: ORNL

Technical Approach

Situ combines anomaly detection and data visualization to provide a distributed, streaming platform for discovery and explanation of suspicious behavior to enhance situation awareness. Our novel approach to anomaly detection is based on unsupervised, probabilistic modeling. Key to our approach is modeling events in different contexts or at multiple scales; each event is modeled and scored by multiple anomaly detectors to identify different kinds of anomalous behavior. Situ is designed to scale to extremely high data rates on commodity hardware — hundreds of thousands of events per second.

Technology Transition

Situ is deployed in the ORNL Security Operations Center, where it processes 500 million flows per day. The system was a 2018 R&D 100 Finalist, holds two patents, and is currently licensed to U2opia, a consortium of technology executives with extensive experience in industry and defense.

Benefits

- Reduces large volumes of raw network data to a manageable number of events for human domain experts to examine
- Highlights suspicious activity that existing signature-based discovery systems cannot detect
- Enables operators to find novel attacks, insider threats, policy violations, and misconfigurations
- Provides visualization, scoring, reporting, and context to help operators understand *why* something is anomalous
- Requires no labeled training data

CONTACT | John Goodall | Augmented Analyst Intelligence Group | jgoodall@ornl.gov

Oak Ridge National Laboratory is managed by UT-Battelle LLC for the US Department of Energy

2022-G00224

OAK RIDGE National Laboratory | U.S. DEPARTMENT OF ENERGY | Office of Science

NATIONAL SECURITY SCIENCES