Background

- Cyber threats emphasize need for collaboration among cyber analysts to develop innovative cyber assessment and defense strategies.
- Empirical research from the “analyst” perspective must be included and is currently limited.

Concept of Operation

- Develop collaborative hands-on workshops focused on cyber forensics, advancement of fundamental theory, models, and algorithms for cybersecurity community.
- Collect and analyze analyst-centric data during workshops to include screenshots, mouse clicks, system calls and tool interaction.
- Establish a collaborative network to enable collection and sharing of datasets and methodologies with partners.

Participants

- Open to all government, academia, and industry with interest in cybersecurity assessment and analysis.

Collaborative Focus

- Target cybersecurity research problems by leveraging empirical data from the analyst viewpoint along with the defender viewpoint.
- Improve security evaluation, remediation, and defense capabilities.
- Identify cross-domain vulnerabilities, potential impacts, and remediation strategies in systems and networks.

Assessment & Analysis Tools and Research

- Visualization
- Machine Learning
- Big Data
- HPC

Security Challenge Scenarios

- Instrumentation
  - Monitors
  - Loggers
  - Sniffers
  - Detection systems

Benefits

- Notional scenarios for analyst-centric training and analysis.
- Collaboratively developed tools and acquired data.
- Environment with cross-domain academics, professionals, and students.
- Exclusive technical workshops and exercises.
- Opportunities for joint proposals.

Unique Facilities/Capabilities

- A hybrid and portable platform that uses hardware, emulation, and simulation for hosting small to large-scale cybersecurity scenarios.
- Access to cybersecurity experts from operational and academic backgrounds.
- Analyst-centric datasets to enable collaborative, cross-domain empirical-based research.