

HIT-IT Heuristic Identification & Tracking of Insider Threat

Cyberspace Sciences & Information
Intelligence Research (CSIIR) Group

• Problem

– Insider sourced espionage, sabotage, and fraud are the **number one** cyber threat.

- Cost estimates US \$250B/yr resulting from mods of data, security mechs, unauth NW connections, covert channels, physical damage/ destruction including *information extrusion/ exfiltration*.

• Technical Approach

- Identify and model characteristic activities and relationships among cyber assets and players
- Multi-level sensing monitors and profiles host/user, network and enclave behaviors
- Uses Times Series, Bayesian and Hidden Markov models of dependency relationships (e.g., spoofing) combined with supervised learning algorithms (e.g., SVMs)
- Refined by threat behavior assessments for converging to more efficient/effective hierarchical and discrete event models

• Benefit

- Comprehensive list of monitored threat behavior attributes supports insider profiling, deterrence and prevention
- Role-based access control facilitates an *extensible* array of host and network-based sensor capabilities

POCs: Frederick T. Sheldon Ph.D., 865-576-1339 sft@ornl.gov
Robert K. Abercrombie, Ph.D., 865-241-6537 abe@ornl.gov

