Cyber Semantic Account Management Service (C-SAMS)

Project Summary: This project will utilize semantic-based technologies to identify and react to cyber threats from adversaries masquerading as an authorized user to access restricted USTRANSCOM Distribution and Deployment data. Securboration, Inc. proposes to build a monitoring capability that will aid USTRANSCOM in identifying and reacting to the masquerading problem of cyber

attacks perpetrated against its systems where the attacker's goal is to exfiltrate information such as intellectual property or future operational plans. C-SAMS, the Cyber-Semantic Account Management Service, will fit within the future Net-Centric JDDE in that it will not require custom integration with operational systems, will be architected as a service, and existing and/or future cyber monitoring display capabilities will leverage this service in defining the aggregate cyber operational picture. The result of this effort will be a prototype of the models and monitoring service that is ready for transition into operational use at the GCCC. This will provide immediate benefit to USTRANSCOM as it will be more adept at identifying insider cyber threats and as a result can react with appropriate courses of action.
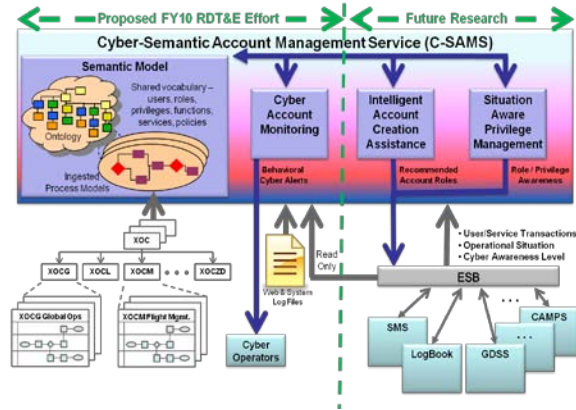
Return on Investment: The immediate cost impact will be the reduction of man-hours required to manually review log data associated with user access using automated notification of suspect communications. Additionally identification of unauthorized access in a more efficient manner will significantly save on man hours required to revalidate users' access and re-baseline of impacted systems. Further benefits of the technology can be realized through the exploitation of the semantic models throughout the USTRANSCOM enterprise.

Duration of project: FY10

Participants: USTRANSCOM J6

Project advocacy (funding or otherwise): USTRANSCOM

Transition: Project will support USTRANSCOM GCCC operations

USTRANSCOM POC office code: TCJ5/4-TT/618-229-1109