The goal of Kudu's proposed effort, named "Internet Cyber Early Warning of Adversary Research and Development (ICEWARD)", is to determine whether it is possible to gain actionable insight into the intent of a cyber-adversary by observing specific behaviors. In particular, the proposers hypothesize that vulnerability researchers make use of public information and resources (such as search engines and websites) that are relevant to their missions, targets, and techniques in such a way that it is possible to glean part of their intent if only we could observe such use and differentiate it from noise (e.g., search engine crawlers). The basis for this hypothesis is both the proposers' own experience as vulnerability researchers and a little-noticed incident in 2010-2011. The proposed approach will investigate the feasibility of creating highly tailored information resources whose access via the public network will be inherently highly correlated with vulnerability research. A second aspect of the proposed work entails the creation of an evaluation methodology for proving or disproving this hypothesis.
Contracting Office Address:
675 North Randolph Street
Arlington, Virginia 22203-2114
United States

Primary Point of Contact:
Mike Frantzen
mikef@kududyn.com

For Help: Federal Service Desk  Accessibility

Return To Opportunities List