Intelligence Advanced Research Projects Activity
IARPA
Creating Advantage through Research and Technology

SCITE

SCIENTIFIC ADVANCES TO CONTINUOUS INSIDER THREAT EVALUATION

INTELLIGENCE VALUE

The SCITE program aimed to advance the U.S. Intelligence Community's ability to detect potential insider threats.

Insider threats are individuals with privileged access within an organization who are, or intend to be, engaged in malicious behaviors such as espionage, sabotage and/or violence. Current practice in insider threat detection relies on "passive indicators" – data sources such as intranet search patterns and financial records that are used to identify indicative behaviors. SCITE research to advance the practice of insider threat detection occured in two thrusts;

- Active Indicators: types of information sent to the workforce that might elicit a distinctive response from insider threats. For example, a stimulus that suggests that certain file-searching behaviors may be noticed is likely to be ignored by a normal user engaged in work-related searches, but may cause a malicious user engaged in espionage to cease certain activities.
- Inference Enterprise Models (IEMs): mathematical models that forecast the accuracy of current and proposed automated systems for detecting insider threats.

A key accomplishment from SCITE was the deployment of active indicators and IEMs by a USG trusted agent and an entity in the commercial sector. The SCITE program ran from March 2016 to December 2019.

PRIME PERFORMERS

- Charles River Analytics
- GE Global research
- Innovative Decisions
- Leidos
- Raytheon BBN Technologies
- University of Central Florida

TESTING AND EVALUATION PARTNERS

- Johns Hopkins University Applied Physics Laboratory
- Massachusetts Institute of Technology Lincoln Laboratory
- Los Alamos National Laboratory

KEYWORDS

- Evidence-based forecasting methods
- Inductive logic
- Probabilistic reasoning

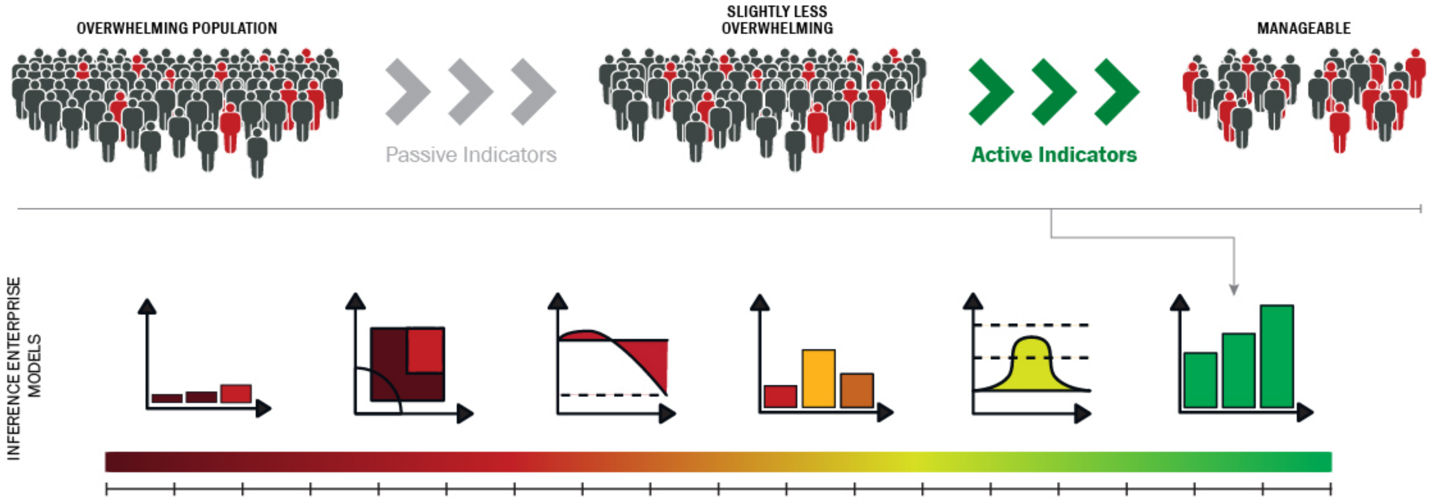

Diagram of SCITE Active Indicators Research

PROGRAM MANAGER

dni-iarpa-info@iarpa.gov
Phone: (301) 243-1995

www.iarpa.gov

@IARPAnews

Latest Revision: 03/08/2022