Technical Detection of Intended Violence Against Self or Others

INSIDER THREAT PROGRAMS

do not know how to detect heightened risk of workplace violence early enough to prevent harm to individuals and mission.

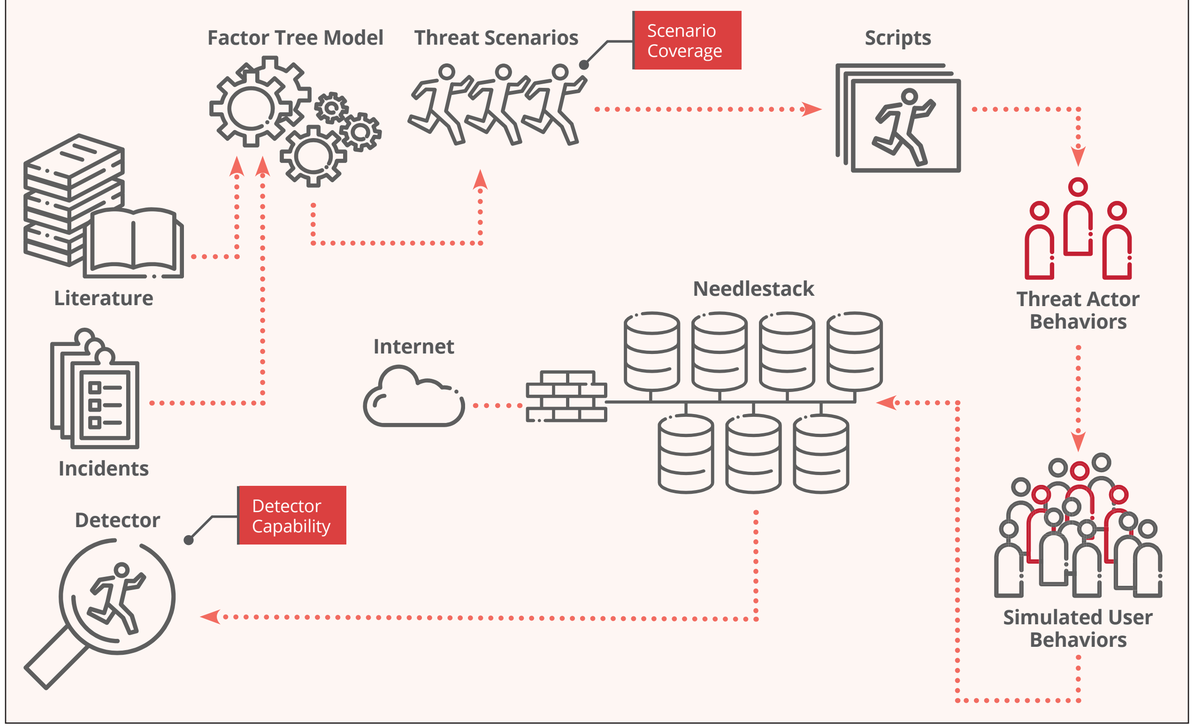
Solution

Develop indicator ontology that maps across the incident lifecycle to online observables and assess technical detection capabilities in a virtual environment

Project Artifacts

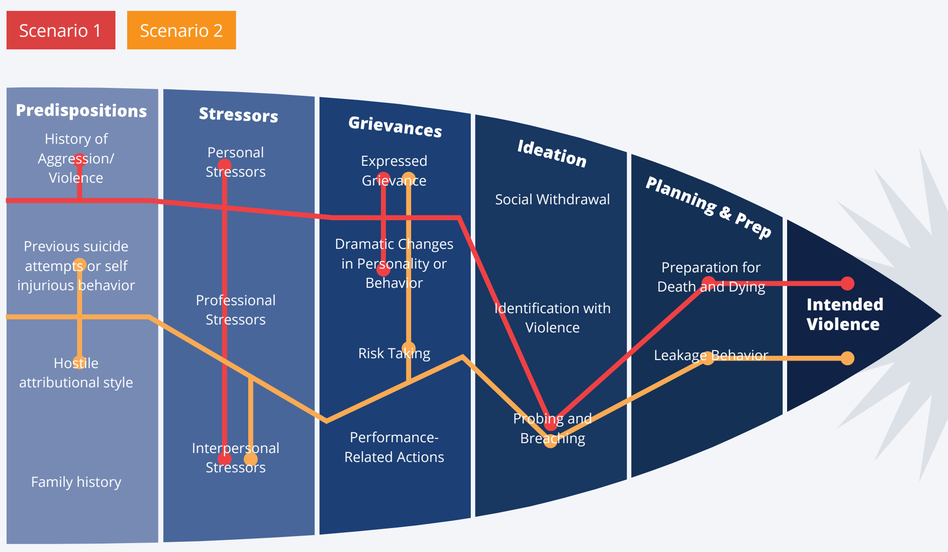
- Scenario Generation Framework
- Coverage and Detection Measures
- Detection Test (Needlestack) Instance
- Report on Balanced Insider Threat Defense

Research Approach

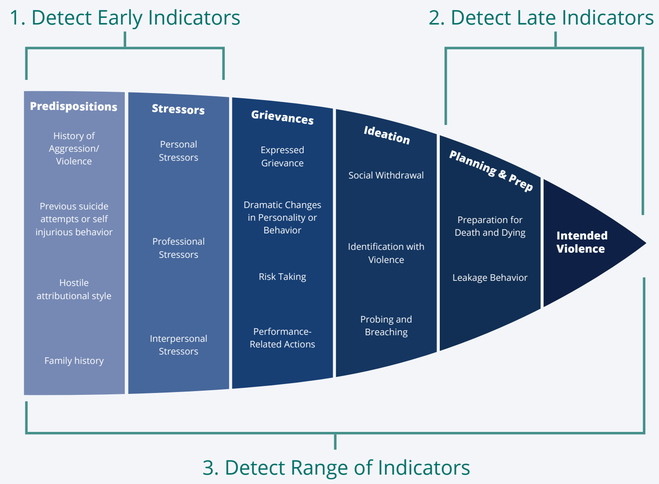


Measures

Scenario Coverage



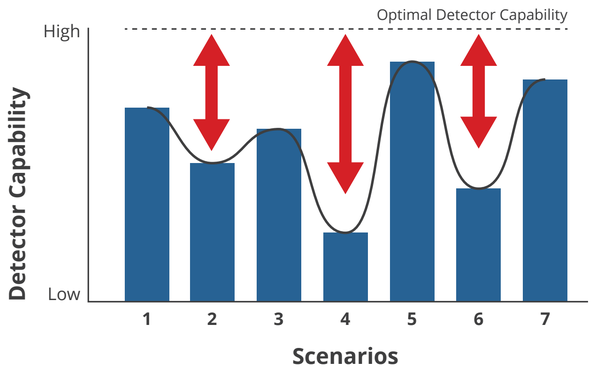
Detector Capability Assessment Criteria



Expected Results

- Human Resources (HR) and other detection tools will be configurable for kinetic threats, though they will not have off-the-shelf capabilities
- Detectors will perform better at detecting late stage than early stage indicators
- False alarms for insider kinetic threats may actually be hits for insider cyber threats

Results Format



Future Work

Calendar Year 2017

- Finish developing scripts for the scenarios
- Run the detector capability assessment trial using Needlestack
- Write final research report on method, measures, insider threat tool testing usage, and findings

Post 2017

- Analyze the applicability of project results to the DoD Insider Threat Program
- Develop technical recommendations for reducing intended harm to self and others in the DoD.

Tracy Cassidy | tmcassidy@cert.org

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM17-0744
Technical Detection of Intended Violence Against Self or Others