

Technical Detection of Intended Violence Against Self or Others

INSIDER THREAT PROGRAMS

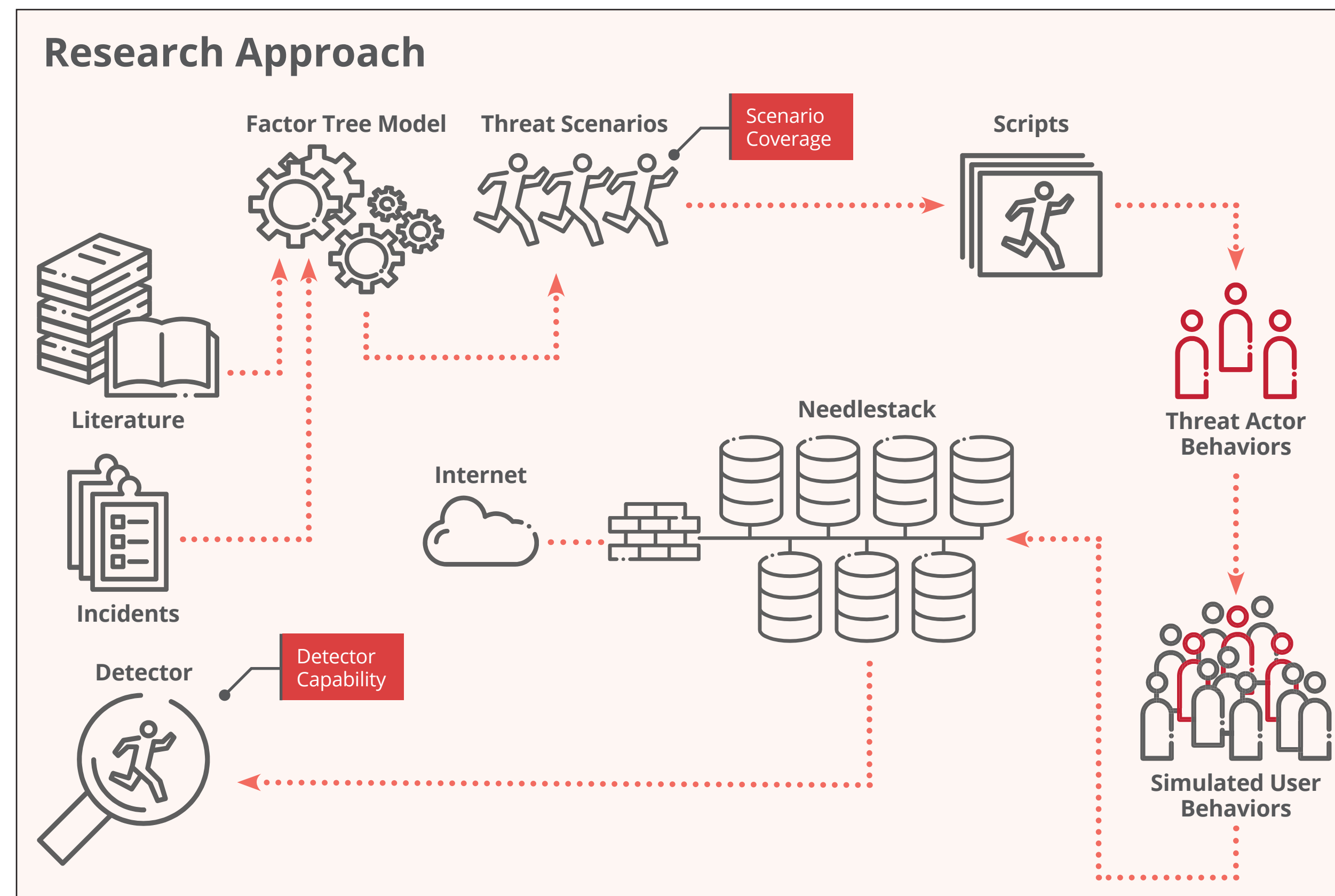
do not know how to detect heightened risk of workplace violence early enough to prevent harm to individuals and mission.

Solution

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

Project Artifacts

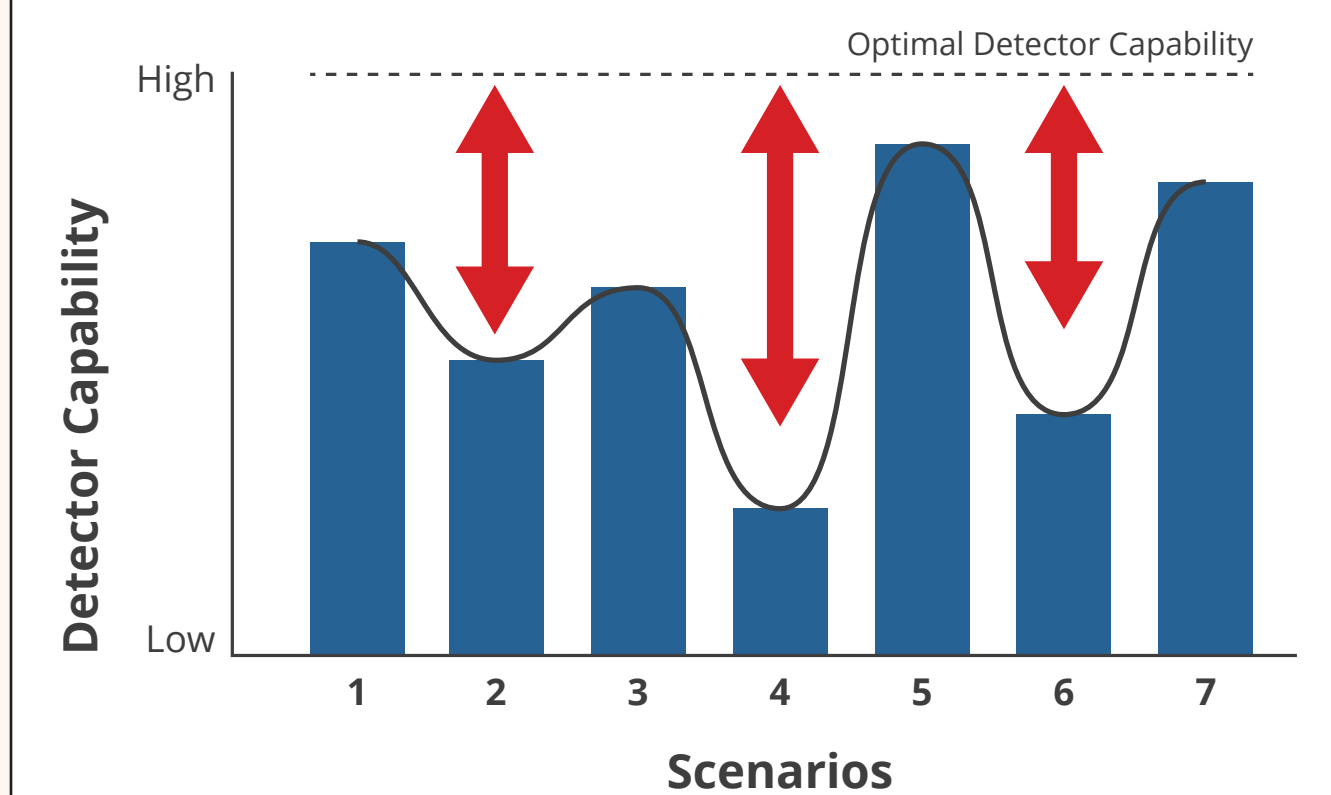
- Scenario Generation Framework
- Coverage and Detection Measures
- Detection Test (Needlestack) Instance
- Report on Balanced Insider Threat Defense



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

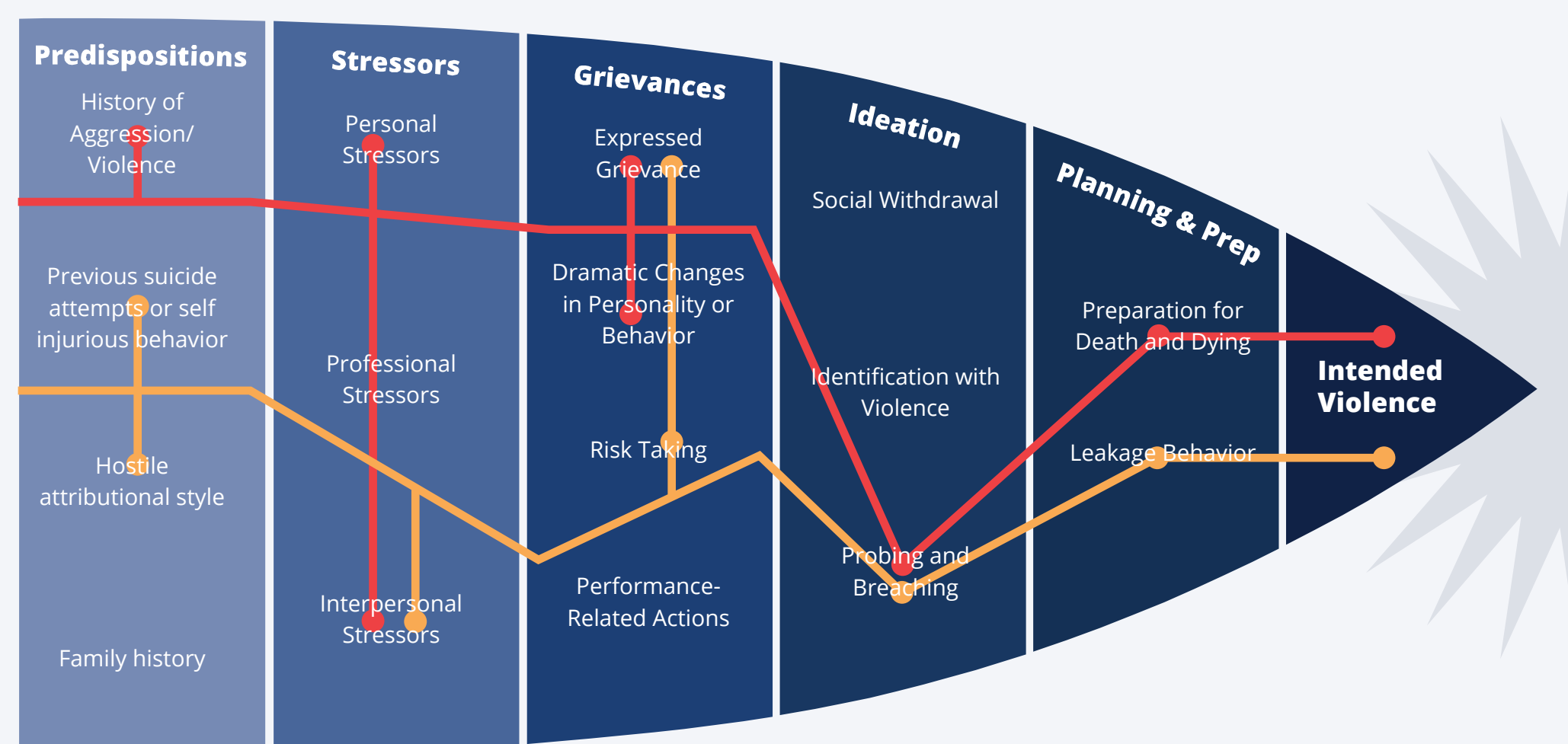
Results Format



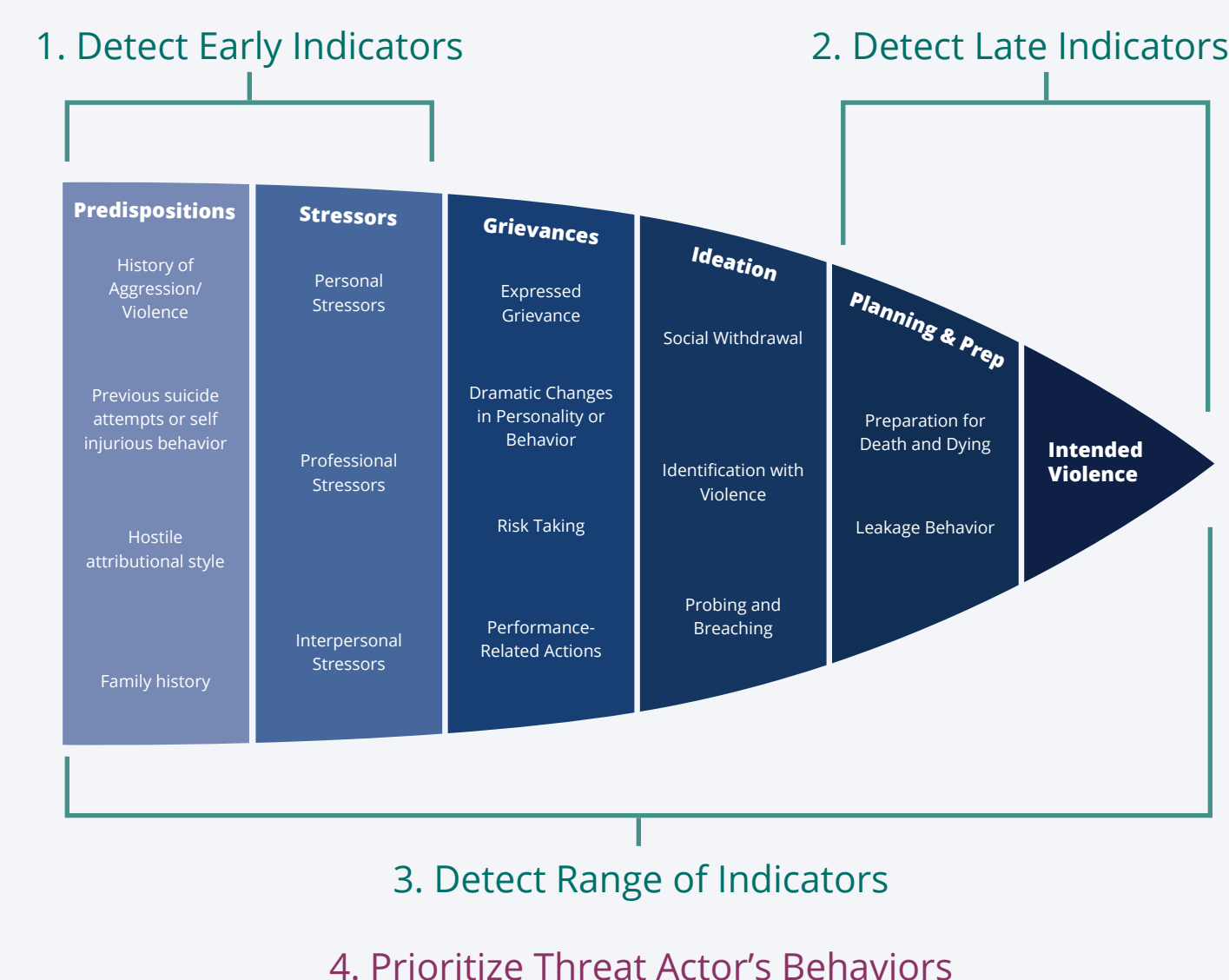
Measures

Scenario Coverage

- Scenario 1
- Scenario 2



Detector Capability Assessment Criteria



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.

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

]

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0744

Technical Detection of Intended Violence Against Self or Others