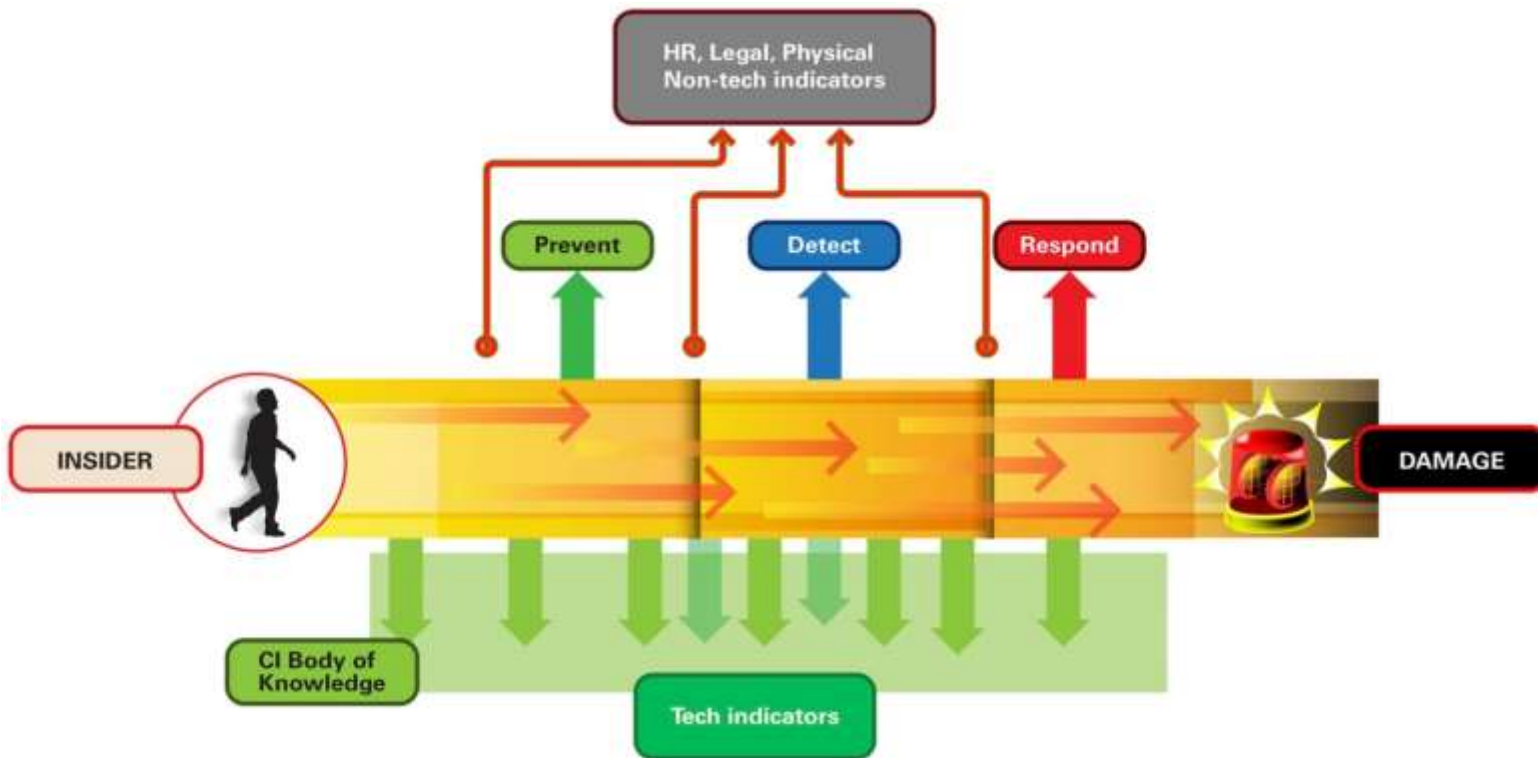


Research Review 2017

# Technical Detection of Harm to Self and/or Others

Tracy Cassidy, Insider Threat Researcher

# CERT Insider Threat Center Objective



Stages of Insider Threat Mitigation

# Project Introduction

## Problem

Lack of early technical detection of increased risk of harming individuals in the workplace

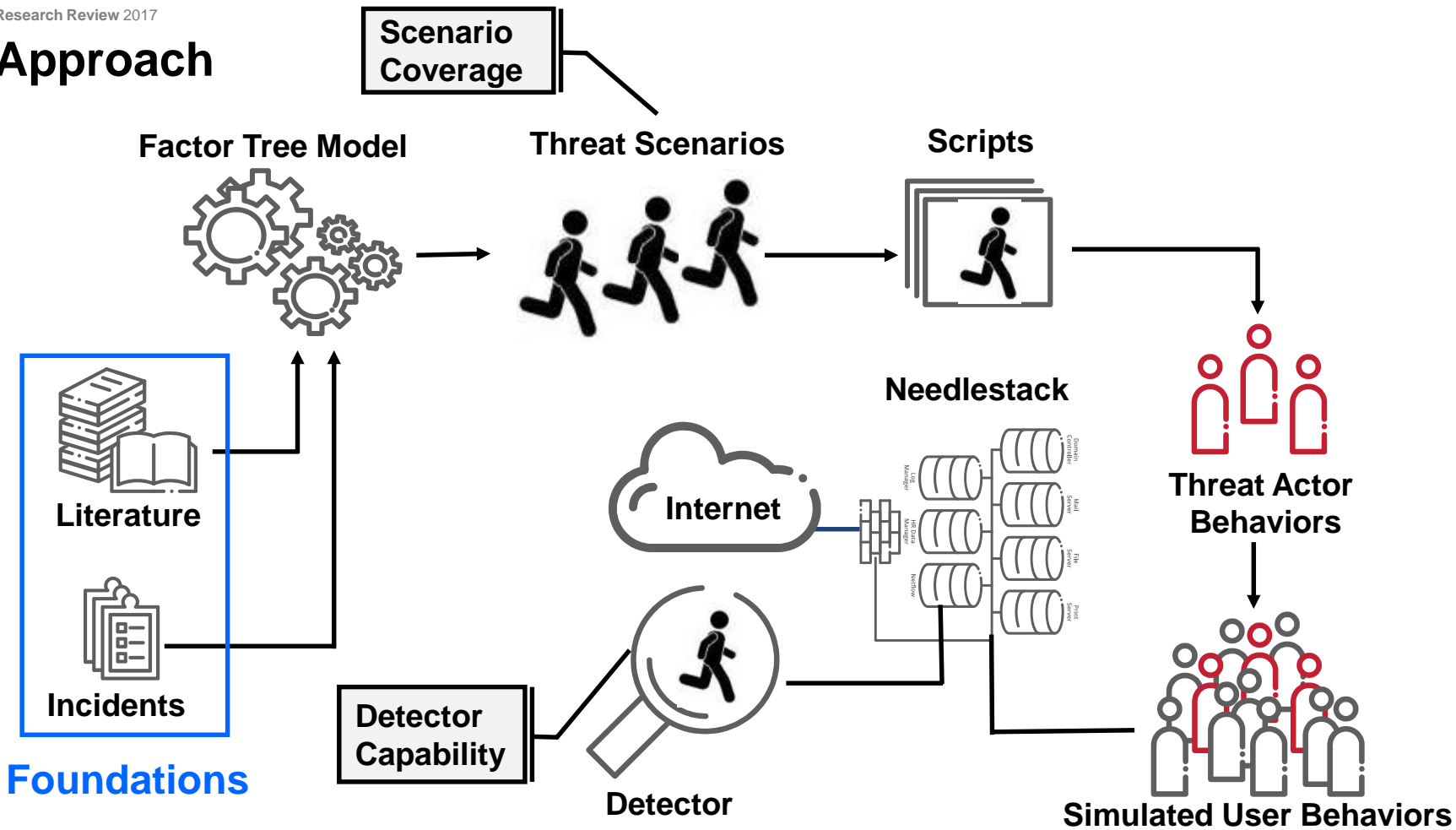
## Solution

- Map validated indicators across the incident pathway to generate prototypical scenarios
- Assess capability of existing tools to detect combinations of indicators in scenarios using online data sources

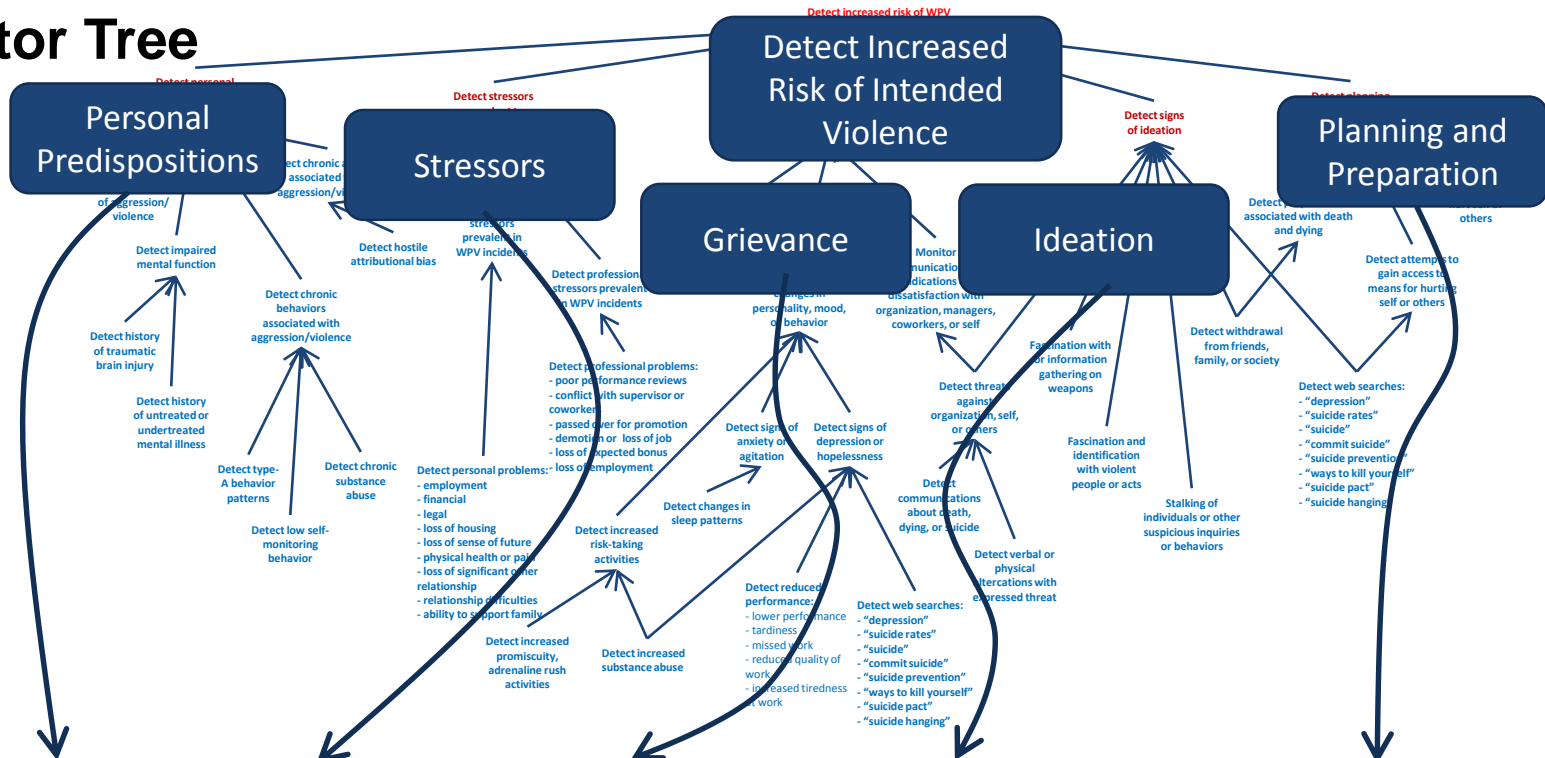
## Detector Testing Environment Used

*Needlestack*: a virtual network-based simulation environment that evolved out of DARPA ADAMS program

# Approach

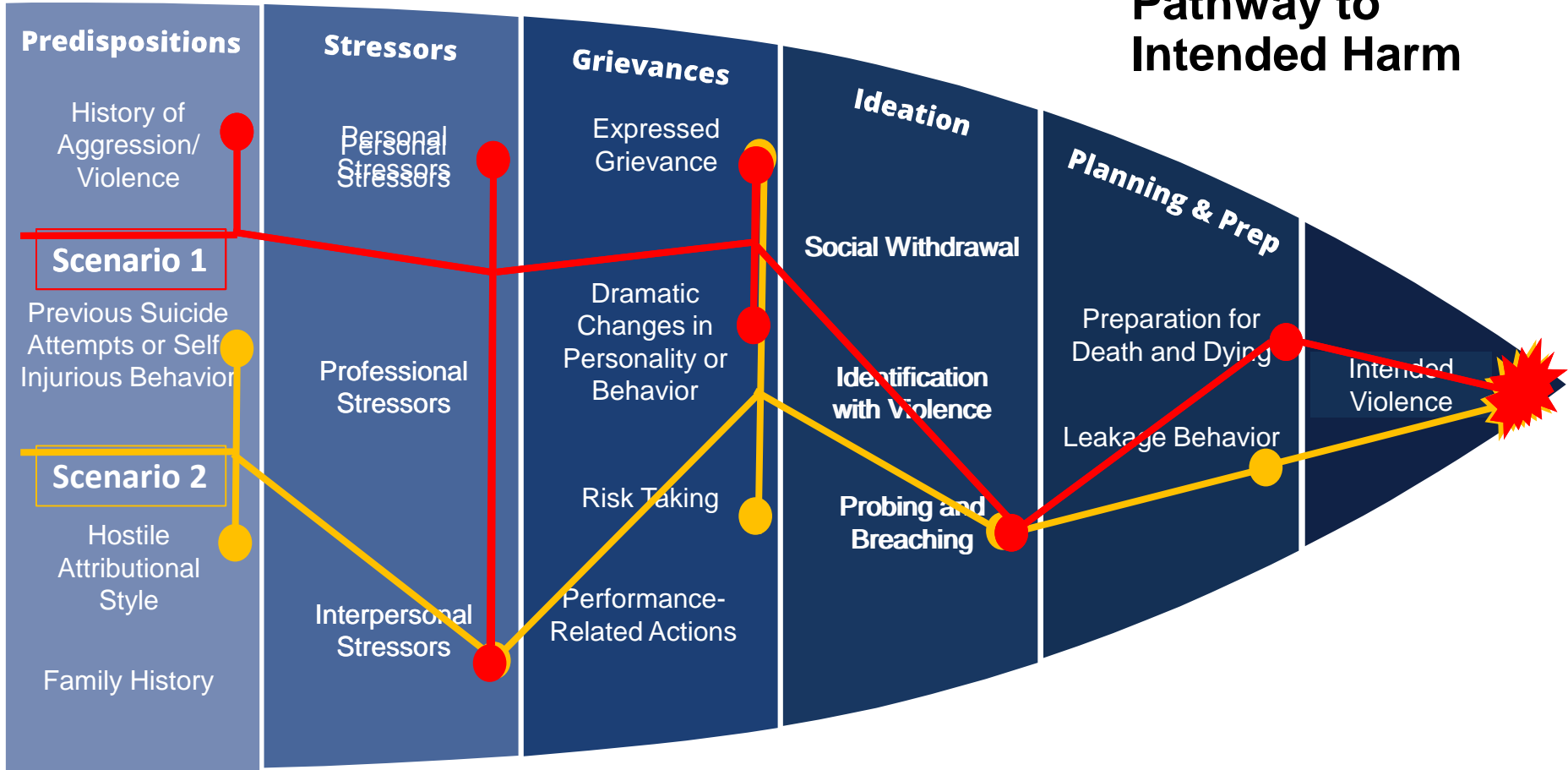


# Factor Tree



Scenario	Predisposition	Stressor	Grievance	Ideation	Planning and Preparation
	History of violence.	Personal and professional	Dissatisfaction with supervisor	Increased drug abuse with threats against supervisor	Web purchase of gun and warning to friendly coworkers to not come to work

# Pathway to Intended Harm



# Mapping Indicators to Data Source — High-Concern Case

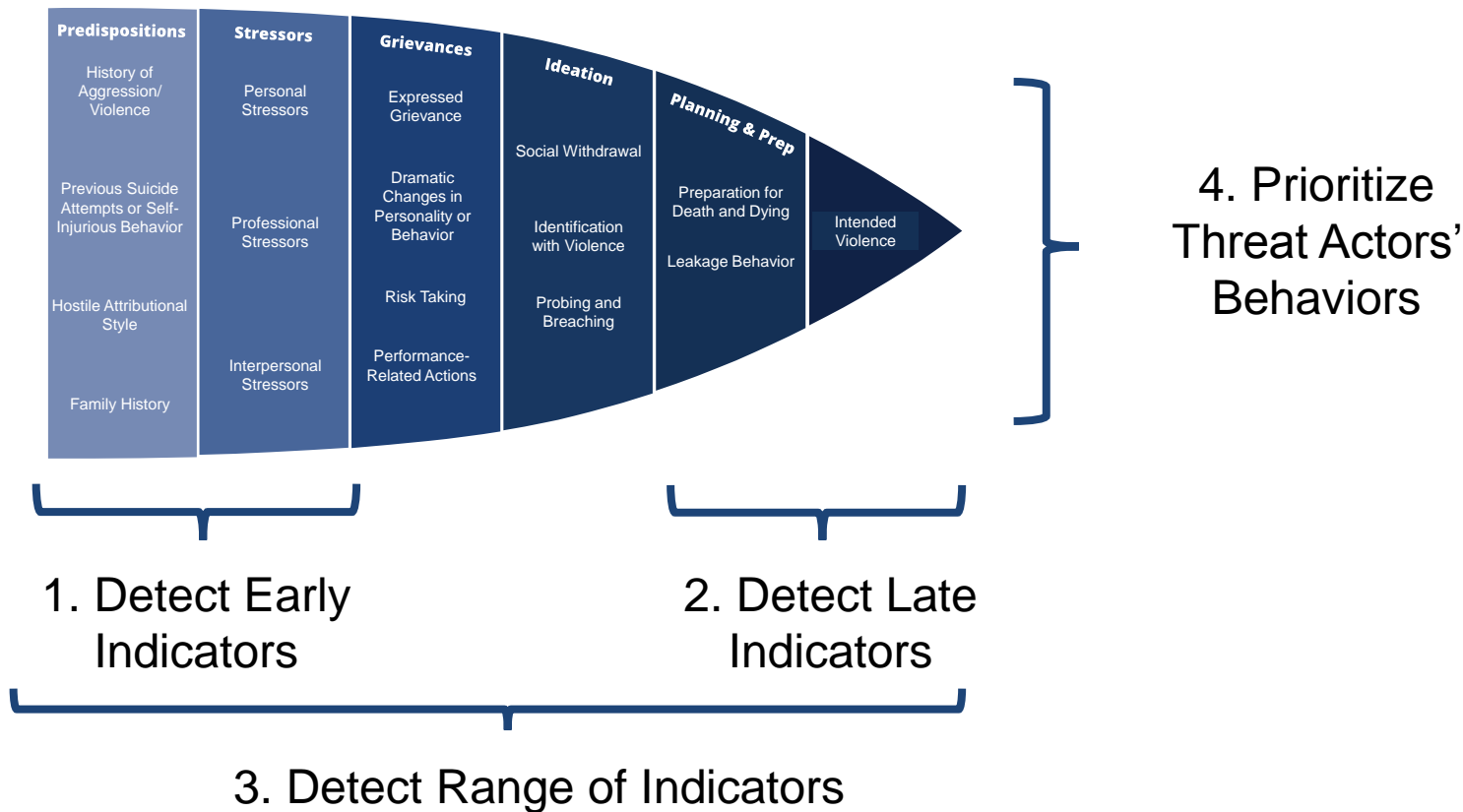
## Indicators

- History of Violence
- Legal Problems
- Loss of Significant Other
- Conflict with Supervisor
- Potential Loss of Employment
- Increased Drinking
- Concerning Web Searches

## Data Sources

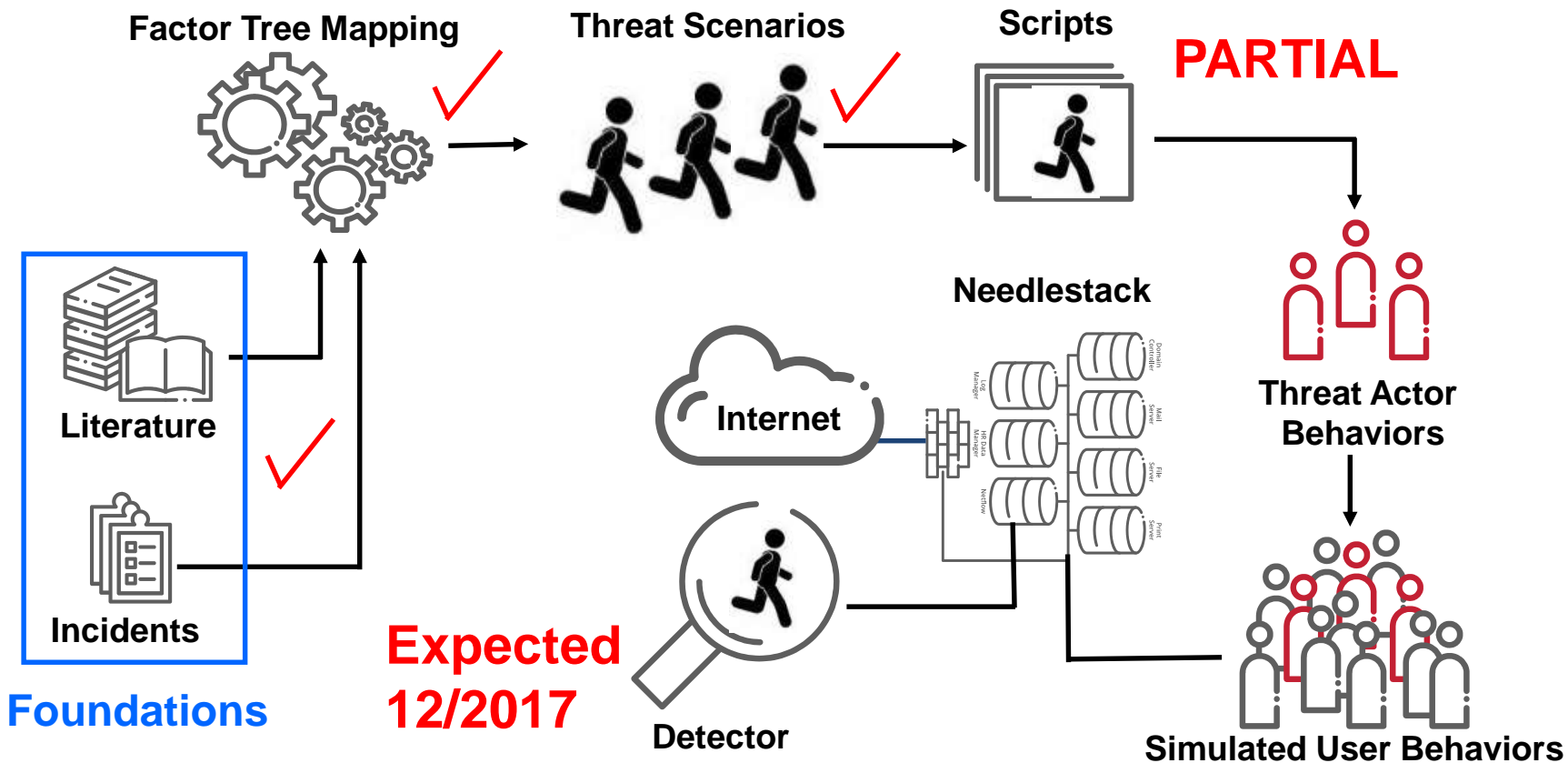
- Criminal History Records
- Required Clearance-Related Events Reporting
- Email/Telephone Records
- Leave Requests
- Sick Time
- Performance Evaluations
- Disciplinary Actions
- Grievance Filings
- Status Change Log
- Physical Security Access Logs
- HTTP Logs

# Detector Capability Assessment Criteria





# Status, Artifacts, and Future Work



# Presenters, Contributors, and Collaborators

## Presenter/Point(s) of Contact

### Tracy Cassidy

Insider Threat Researcher

Email: [tmcassidy@cert.org](mailto:tmcassidy@cert.org)

## SEI Contributors

Andrew Moore

Sarah Miller

Michael Hansell

Carrie Gardner

## External Collaborators

Dr. Jack Rozel, University of Pittsburgh  
Medical Center Psychiatrist

# Questions?

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.

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 use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

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

DM17-0787

# Backup

# Scenario #1- High concern for workplace violence

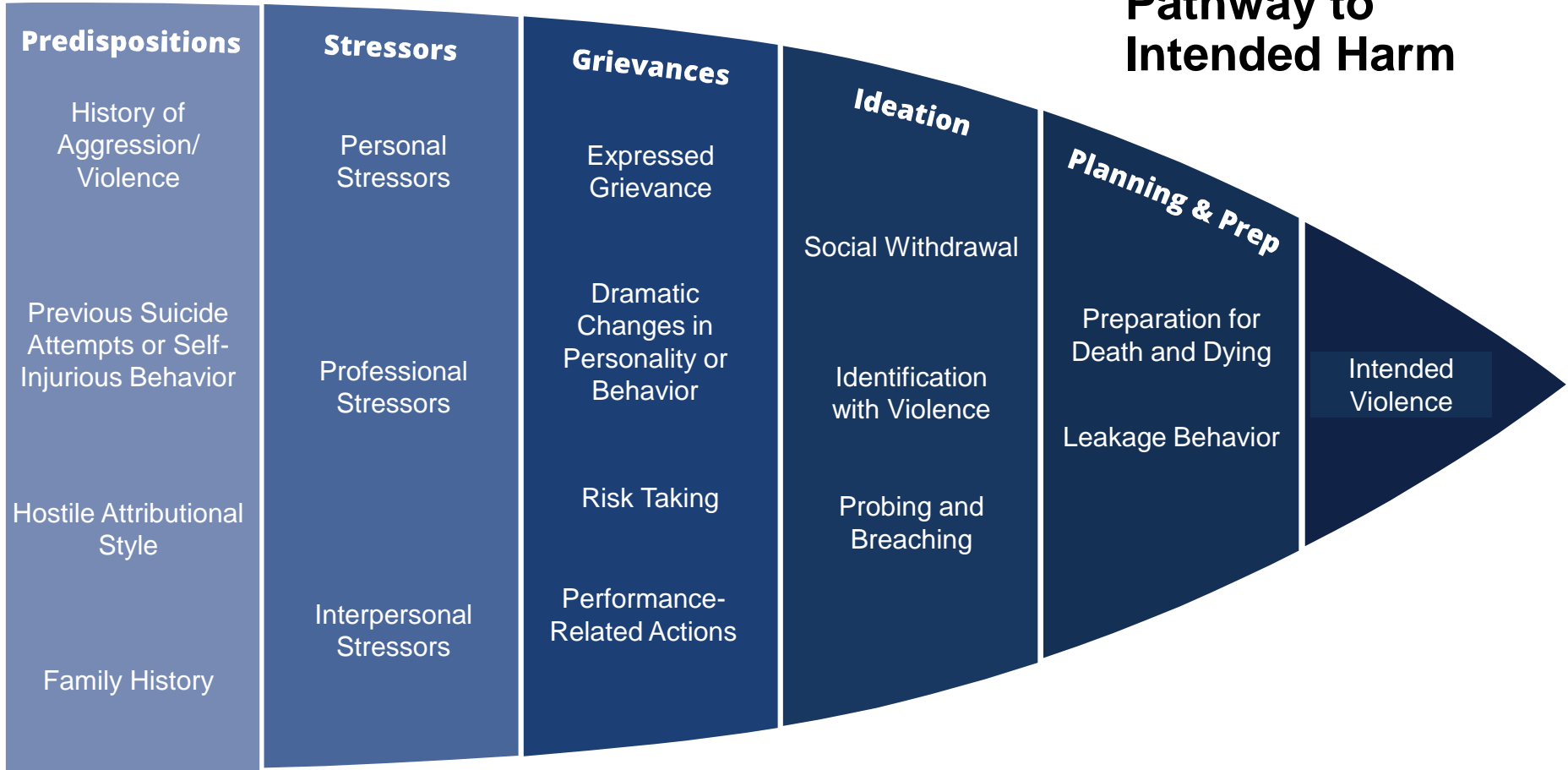


- 33-year old male with a history of violence
- Placed on probation at work due to poor performance
- Two arrests for domestic violence resulting in the loss of his family
- Increased alcohol abuse
- Threats via email to his supervisor
- Externalizing blame
- Human Resources intervention
- Concerning web searches (e.g., how to expedite the sale of a gun)

# Expected Results

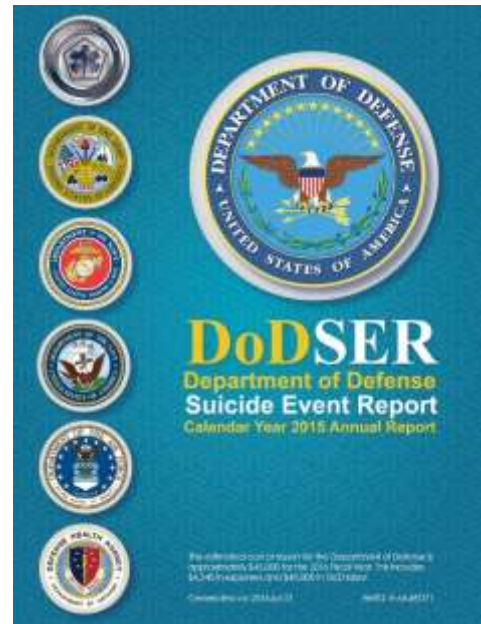
- Human Resources (HR) tools and other detection tools are configurable for kinetic threats, though they do not have off-the-shelf capabilities.
- Detectors perform better at identifying late-stage indicators than early-stage indicators.
- False alarms for insider kinetic threats may actually be hits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

# Pathway to Intended Harm





# DoD Impact of Employee Harm to Self and/or Others



# Artifacts from This Effort

Scenario Generation Framework

Coverage and Detection Measures

Detection Test (Needlestack) Instance

Report on Balanced Insider Threat Defense



# Future Work

## Calendar Year 2017

- Finish developing scripts for the scenarios
- Run the detector capability assessment trial using the CERT Insider Threat Tool Testing Environment.
- Write the final research report on the 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.

# Form of Results

