Research Review 2017

Technical Detection of Harm to Self and/or Others

Tracy Cassidy, Insider Threat Researcher

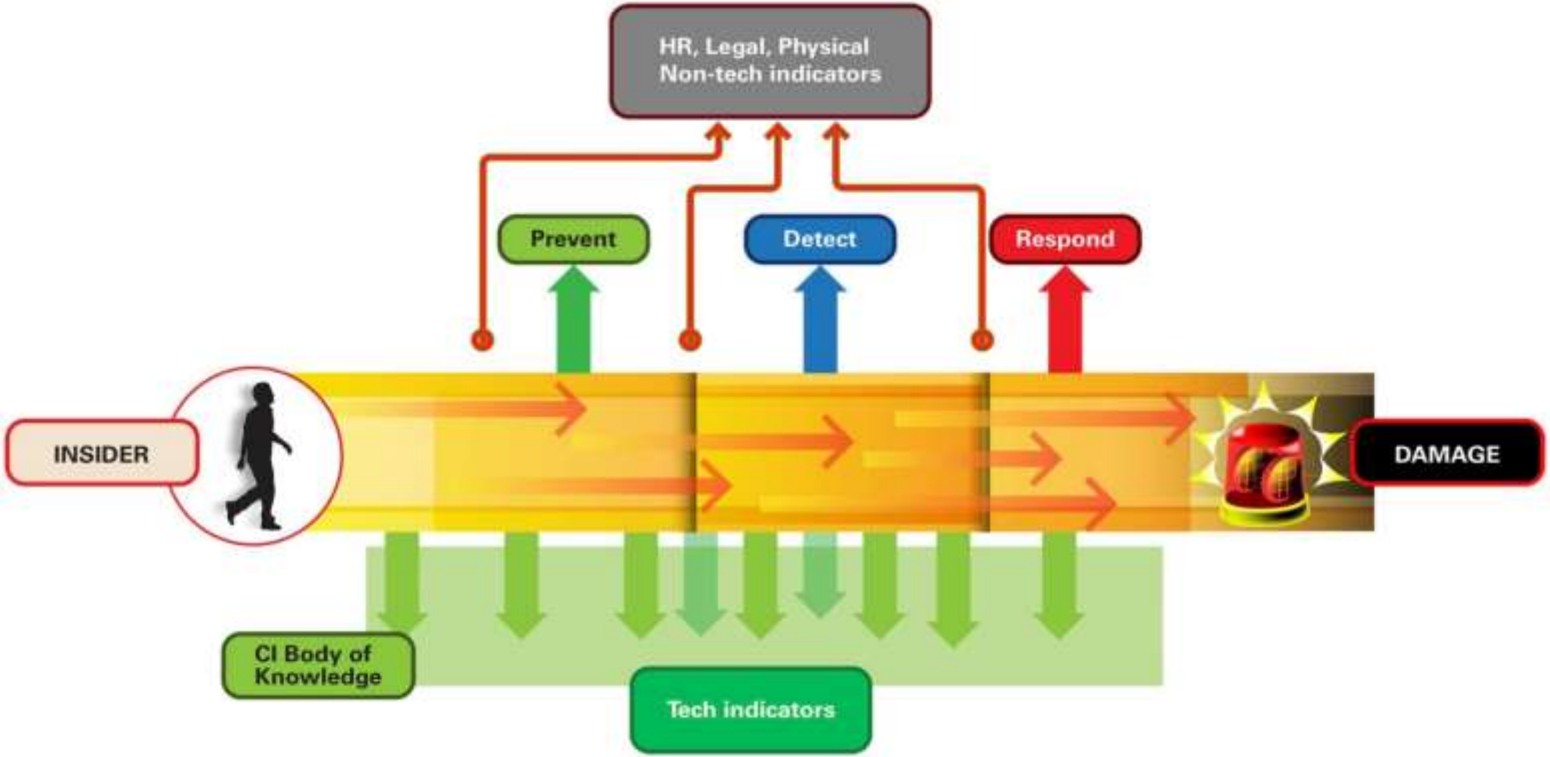
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

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.

DM17-0787

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

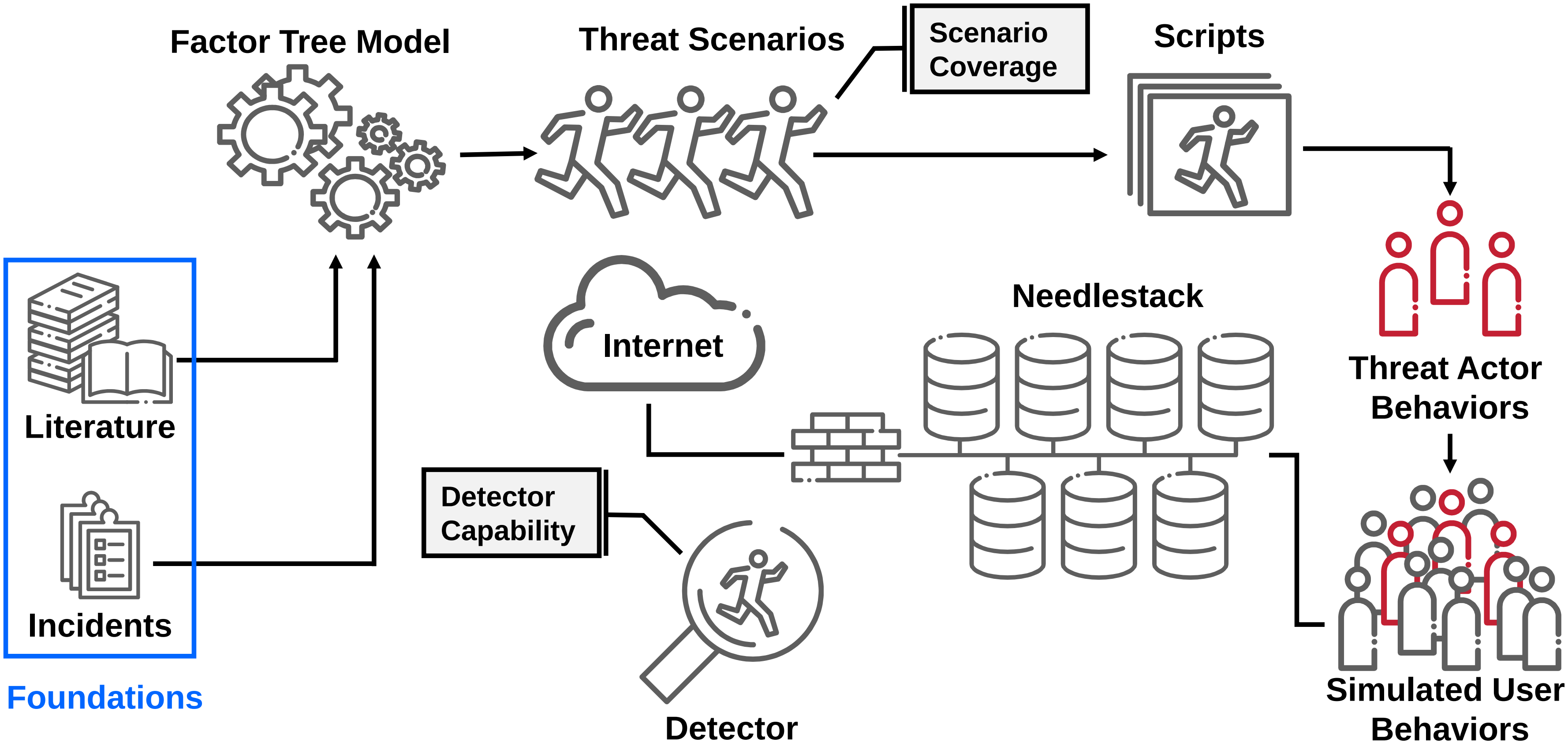
Solution

- 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

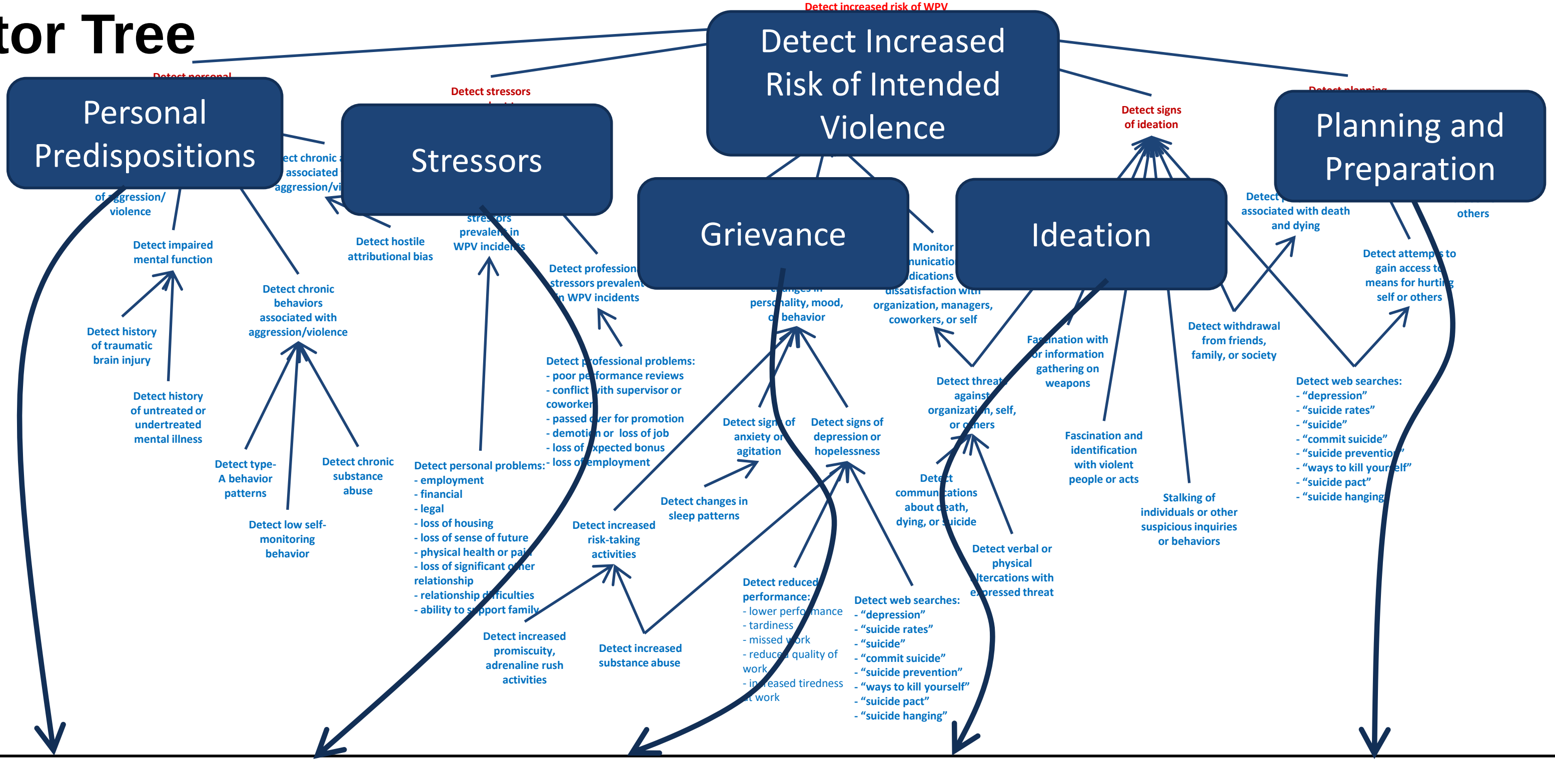
Detector Testing Environment Used

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

Approach


Factor Tree Model
Threat Scenarios
Scenario Coverage
Scripts
Literature
Incidents
Foundations
Internet
Needlestack
Threat Actor Behaviors
Detector Capability
Detector
Simulated User Behaviors

Factor Tree


Detect increased risk of WPV
Detect Increased Risk of Intended Violence
Detect personal
Personal Predispositions
Detect stressors
Stressors
Grievance
Detect signs of ideation
Ideation
Detect planning
Planning and Preparation
ect chronic associated aggression/vi
of aggression/ violence
Detect impaired mental function
Detect history of traumatic brain injury
Detect history of untreated or undertreated mental illness
Detect chronic behaviors associated with aggression/violence
Detect type-A behavior patterns
Detect chronic substance abuse
Detect low self-monitoring behavior
Detect hostile attributional bias
stressors prevalent in WPV incidents
Detect personal problems:
- employment
- financial
- legal
- loss of housing
- loss of sense of future
- physical health or pain
- loss of significant other relationship
- relationship difficulties
- ability to support family
Detect professional stressors prevalent in WPV incidents
Detect professional problems:
- poor performance reviews
- conflict with supervisor or coworker
- passed over for promotion
- demotion or loss of job
- loss of expected bonus
- loss of employment
Detect increased risk-taking activities
Detect increased promiscuity, adrenaline rush activities
Detect increased substance abuse
changes in personality, mood, or behavior
Detect signs of anxiety or agitation
Detect signs of depression or hopelessness
Detect changes in sleep patterns
Detect reduced performance:
- lower performance
- tardiness
- missed work
- reduced quality of work
- increased tiredness at work
Detect web searches:
- “depression”
- “suicide rates”
- “suicide”
- “commit suicide”
- “suicide prevention”
- “ways to kill yourself”
- “suicide pact”
- “suicide hanging”
Monitor communications indications dissatisfaction with organization, managers, coworkers, or self
Detect threats against organization, self, or others
Detect communications about death, dying, or suicide
Detect verbal or physical altercations with expressed threat
Fascination with or information gathering on weapons
Fascination and identification with violent people or acts
Stalking of individuals or other suspicious inquiries or behaviors
Detect withdrawal from friends, family, or society
Detect associated with death and dying
Detect web searches:
- “depression”
- “suicide rates”
- “suicide”
- “commit suicide”
- “suicide prevention”
- “ways to kill yourself”
- “suicide pact”
- “suicide hanging”
Detect attempts to gain access to means for hurting self or others
others

Scenario

Predisposition
History of
 violence.

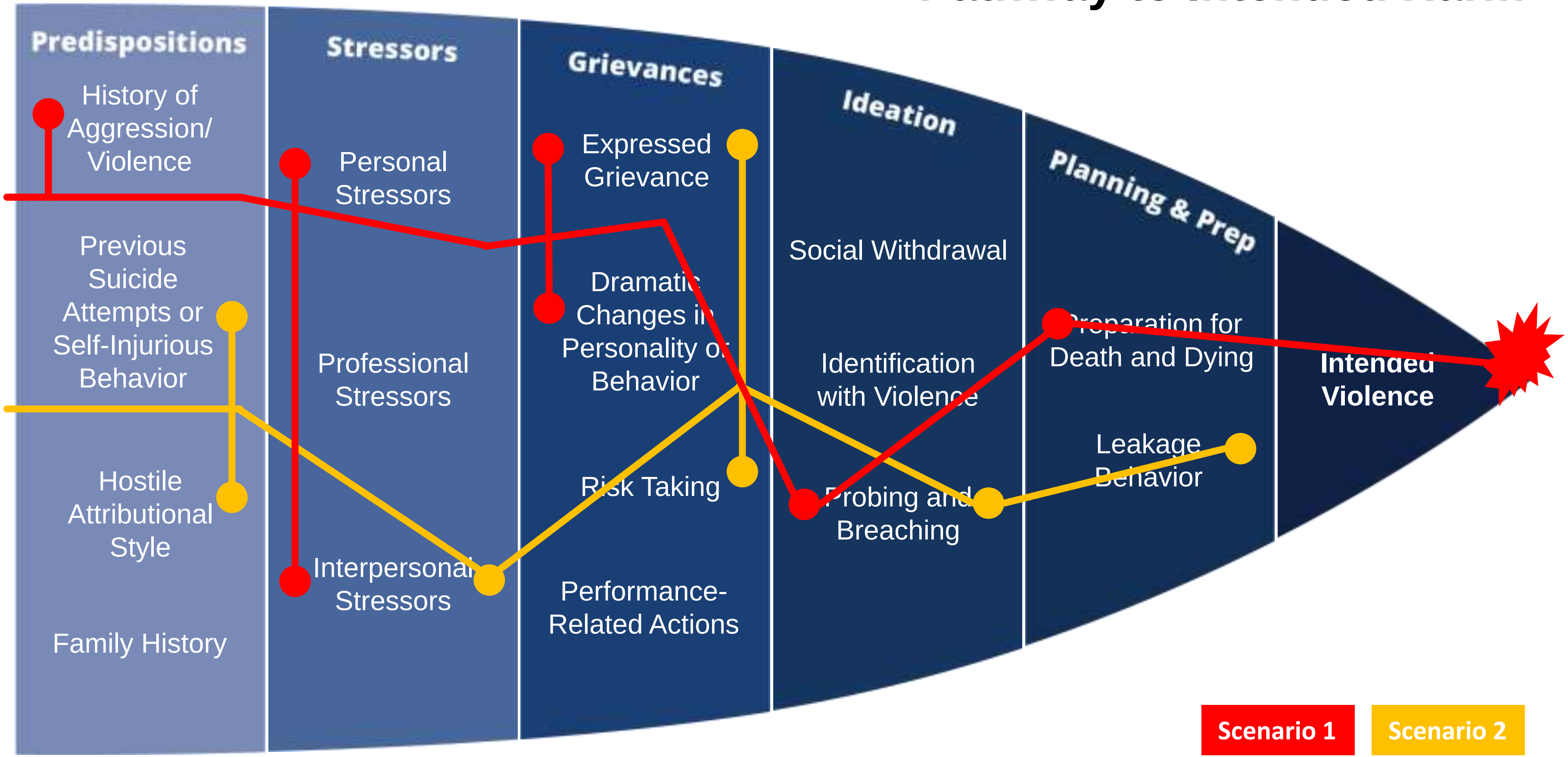
Stressor
Personal and
professional

Grievance
Dissatisfaction
with supervisor

Ideation
Increased drug
abuse with threats
against supervisor

Planning and Preparation
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

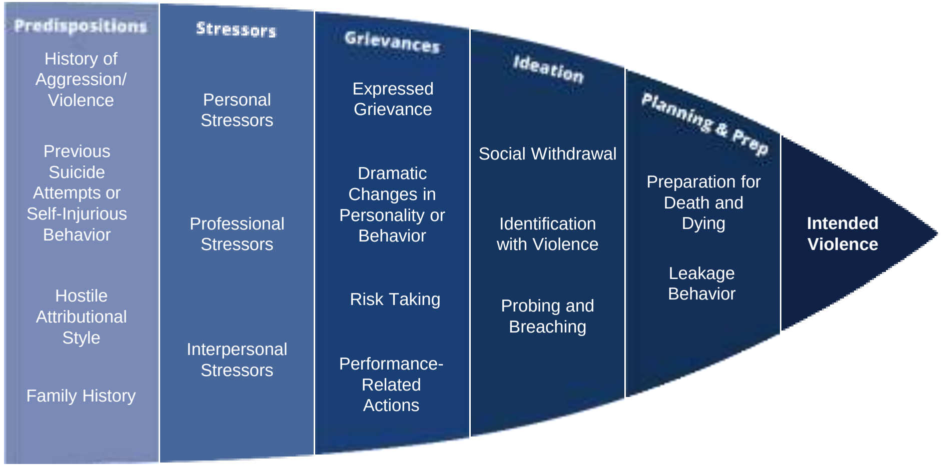
Indicators

- 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

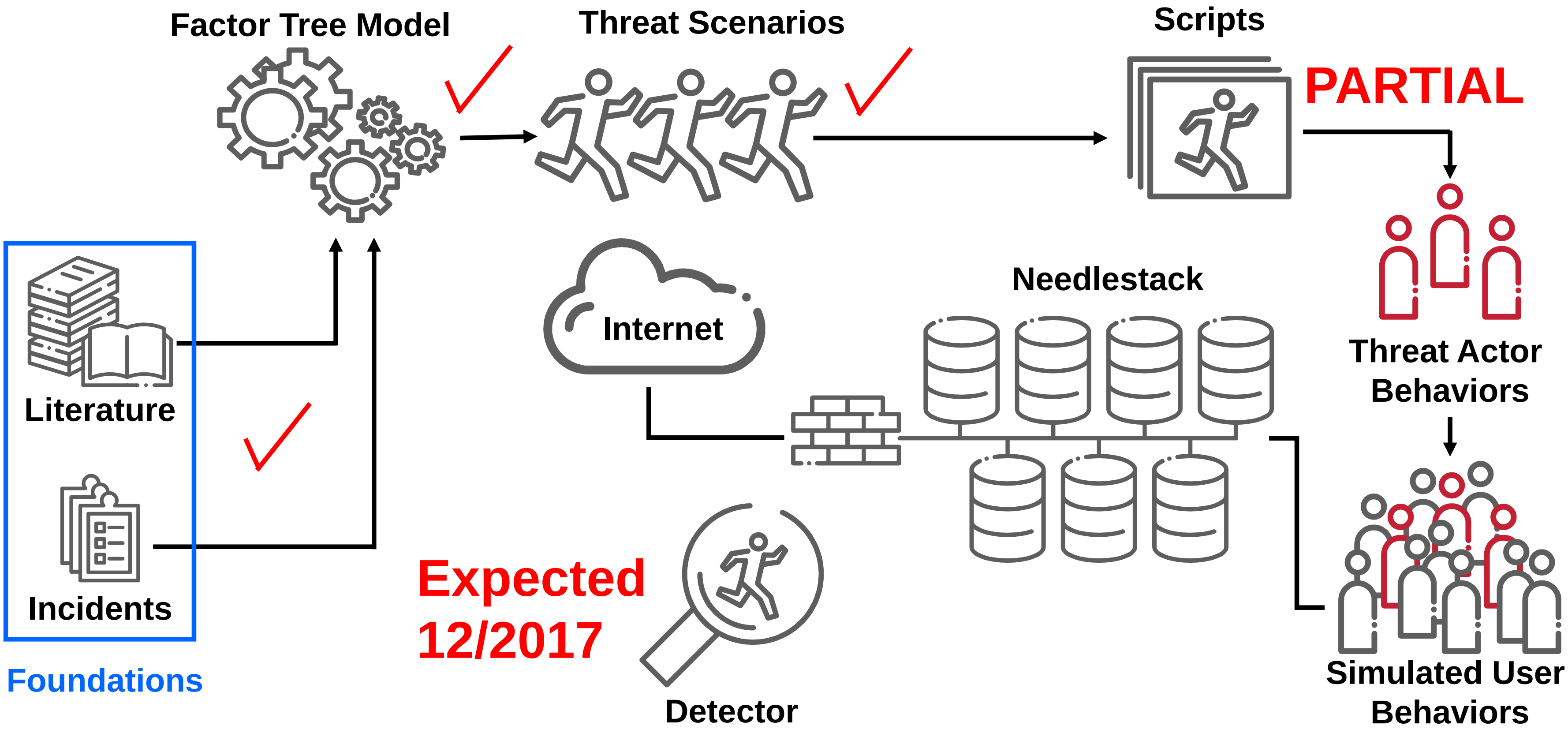

Predispositions
History of Aggression/ Violence
Previous Suicide Attempts or Self-Injurious Behavior
Hostile Attributional Style
Family History
Stressors
Personal Stressors
Professional Stressors
Interpersonal Stressors
Grievances
Expressed Grievance
Dramatic Changes in Personality or Behavior
Risk Taking
Performance-Related Actions
Ideation
Social Withdrawal
Identification with Violence
Probing and Breaching
Planning & Prep
Preparation for Death and Dying
Leakage Behavior
Intended Violence

4. Prioritize Threat Actors' Behaviors

1. Detect Early Indicators

2. Detect Late Indicators

3. Detect Range of Indicators



Factor Tree Model

✓

Threat Scenarios

✓

Scripts

PARTIAL

Literature

✓

Incidents

Foundations

Internet

Needlestack

Threat Actor Behaviors

Expected 12/2017

Detector

Simulated User Behaviors

Presenters, Contributors, and Collaborators

Presenter/Point(s) of Contact

Tracy Cassidy

Insider Threat Researcher

Email: tmcassidy@cert.org

SEI Contributors

Andrew Moore

Sarah Miller

Michael Hansell

Carrie Gardner

External Collaborators

Dr. Jack Rozel, University of Pittsburgh Medical Center Psychiatrist