Technical Detection of Harm to Self and/or Others

Tracy Cassidy, Insider Threat Researcher
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.


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 → Factor Tree Model → Threat Scenarios

Incidents → Threat Actor Behaviors

Foundations

Internet

Needlestack

Detector Capability

Detector

Simulated User Behaviors
Detect increased risk of WPV

Stressors
- 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 increased risk-taking activities
- Detect reduced performance:
  - Lower performance
  - Tardiness
  - Missed work
  - Reduced quality of work
  - Increased tardiness
- Detect increased substance abuse
- Detect increased promiscuity, adrenaline rush activities
- Detect hostile attributional bias
- Detect chronic behaviors associated with aggression/violence

Grievance
- 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 of WPV incidents
- Detect professional predictors of WPV incidents
- Detect hostile attributional bias
- Detect stressors prevalent to WPV incidents
- Detect personal stressors prevalent in WPV incidents
- Detect increased risk - taking activities
- Detect changes in sleep patterns
- Detect signs of anxiety or agitation

Ideation
- Detect signs of depression or hopelessness
- Detect communications about death, dying, or suicide
- Detect plans and preparation
- Detect verbal or physical altercations with expressed threat
- Detect increased substance abuse
- Detect reduced performance
- Detect hostile attributional bias
- Detect chronic behaviors associated with aggression/violence
- Detect increased risk of WPV
- Detect signs of ideation

Planning and Preparation
- Detect withdrawal from friends, family, or society
- Detect web searches:
  - "depression"
  - "suicide rates"
  - "suicide"
  - "commit suicide"
  - "suicide preventing"
  - "ways to kill yourself"
  - "suicide post"
  - "suicide hanging"
- Detect planning and preparation
- Detect verbal or physical altercations with expressed threat
- Detect stressors associated with death and dying
- Detect stressors associated with death and dying

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

**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**

**Scenario 1**

**Scenario 2**
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

1. Detect Early Indicators
2. Detect Late Indicators
3. Detect Range of Indicators
4. Prioritize Threat Actors’ 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