



# Technical Detection Methods for Insider Risk Management

Dan Costa

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Document Markings

Copyright 2020 Carnegie Mellon University.

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.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

**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.**

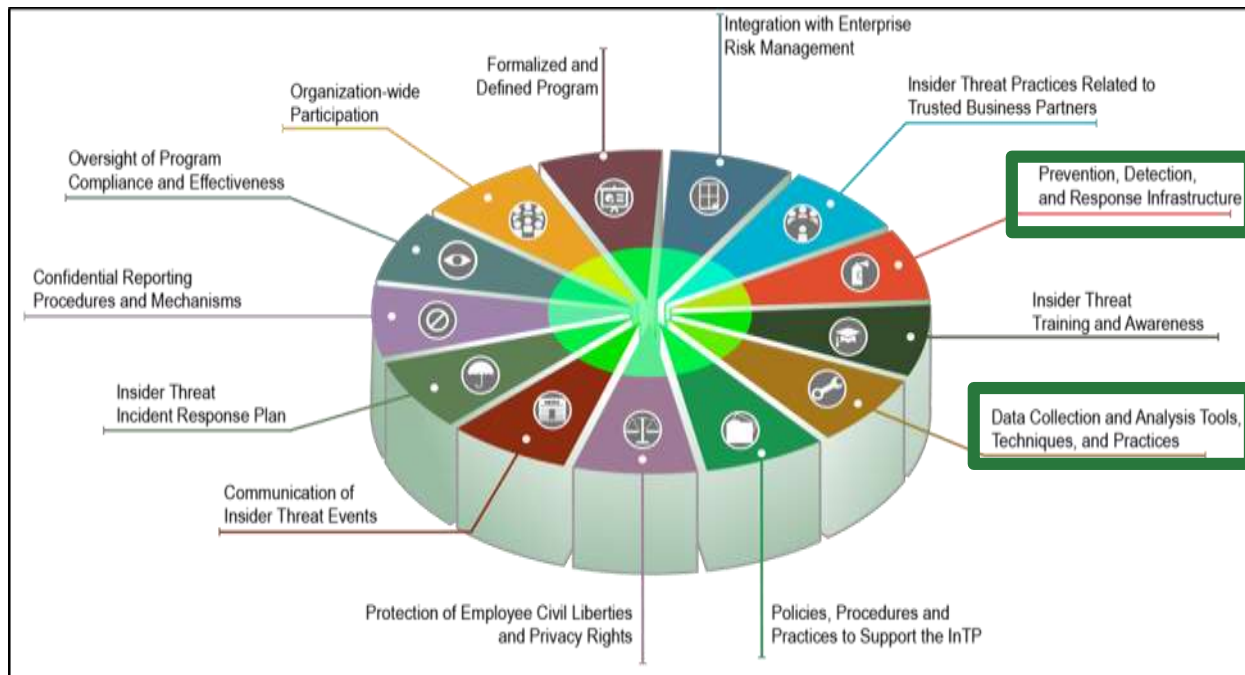
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

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.













DM20-0846

# An Overview of Insider Threat Program Components

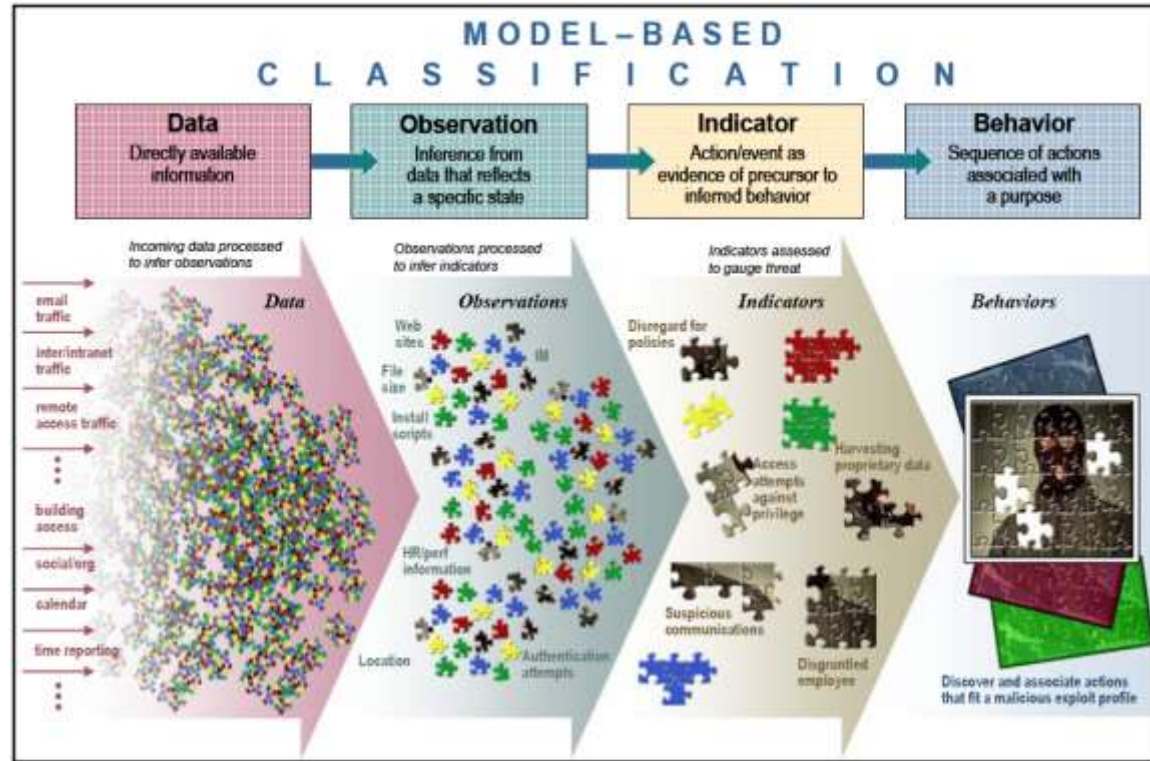


Focus of Today's Talk

# Applicable Best Practices from the CERT Common Sense Guide to Mitigating Insider Threats

1 - Know and protect your critical assets. 	12 - Deploy solutions for monitoring employee actions and correlating information from multiple data sources. 
2 - Develop a formalized insider threat program.	13 - Monitor and control remote access from all endpoints, including mobile devices. 
3 - Clearly document and consistently enforce policies and controls. 	14 - Establish a baseline of normal behavior for both networks and employees. 
4 - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	15 - Enforce separation of duties and least privilege. 
5 - Anticipate and manage negative issues in the work environment.	16 - Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities. 
6 - Consider threats from insiders and business partners in enterprise-wide risk assessments.	17 - Institutionalize system change controls. 
7 - Be especially vigilant regarding social media.	18 - Implement secure backup and recovery processes.
8 - Structure management and tasks to minimize unintentional insider stress and mistakes.	19 - Close the doors to unauthorized data exfiltration. 
9 - Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees. 	20 - Develop a comprehensive employee termination procedure.
10 - Implement strict password and account management policies and practices. 	21 - Adopt positive incentives to align the workforce with the organization.
11 - Institute stringent access controls and monitoring policies on privileged users. 	<a href="http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=540644">http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=540644</a>

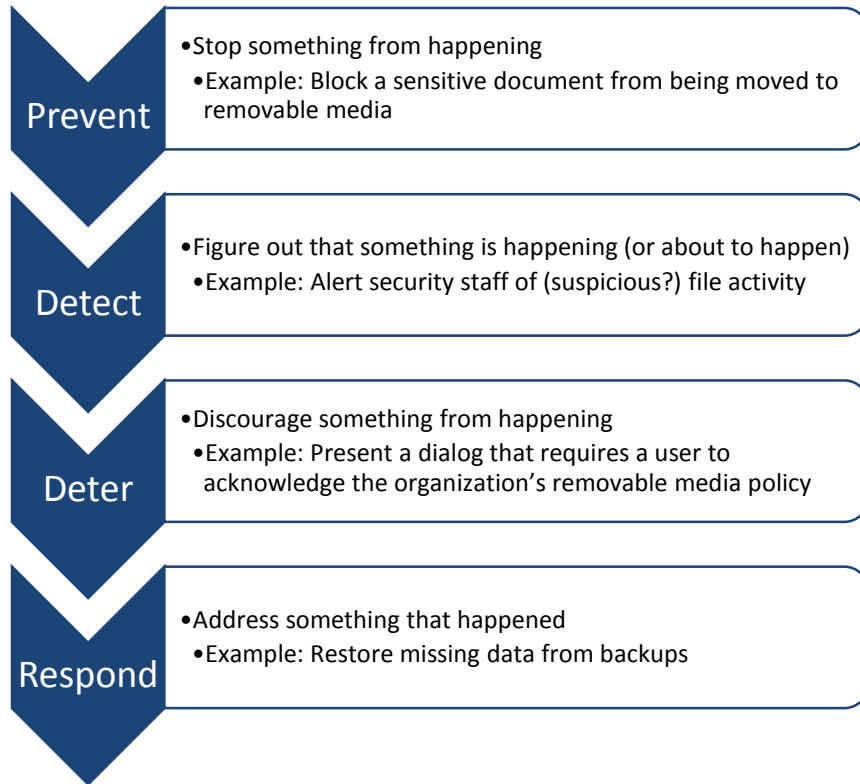
# A Conceptual Model



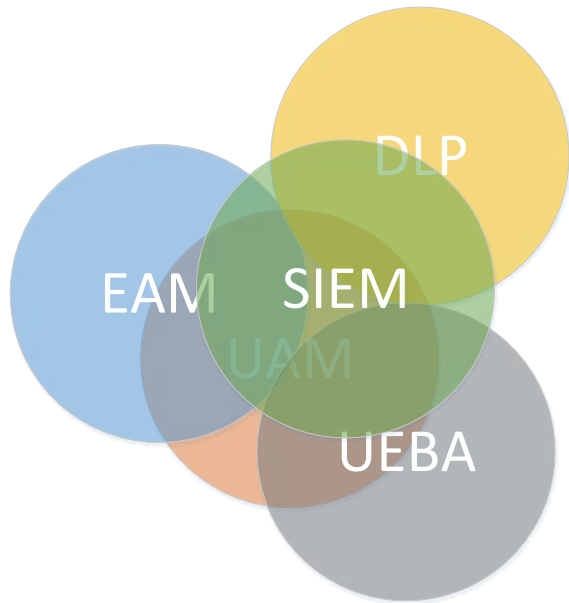
Source: Greitzer, et al., "Predictive Modeling for Insider Threat Mitigation," PNNL-SA-65204, April 2009.

# Insider Threat Tools Vary In Features and Functions

Auditing Host-based Activity	Auditing Network-based Activity	Preventing Data from Leaving Authorized Locations
Preserving Forensic Artifacts	Data Visualization	Rule-Based Alerting
Identity Management / Access Management	Data Correlation / Entity Resolution	Anomaly Detection
Machine Learning	Text Analysis	Risk Scoring
Case / Incident Management	Data Masking / Anonymization	... And More ...



# Finding The Right Tools For The Job Can Be Challenging



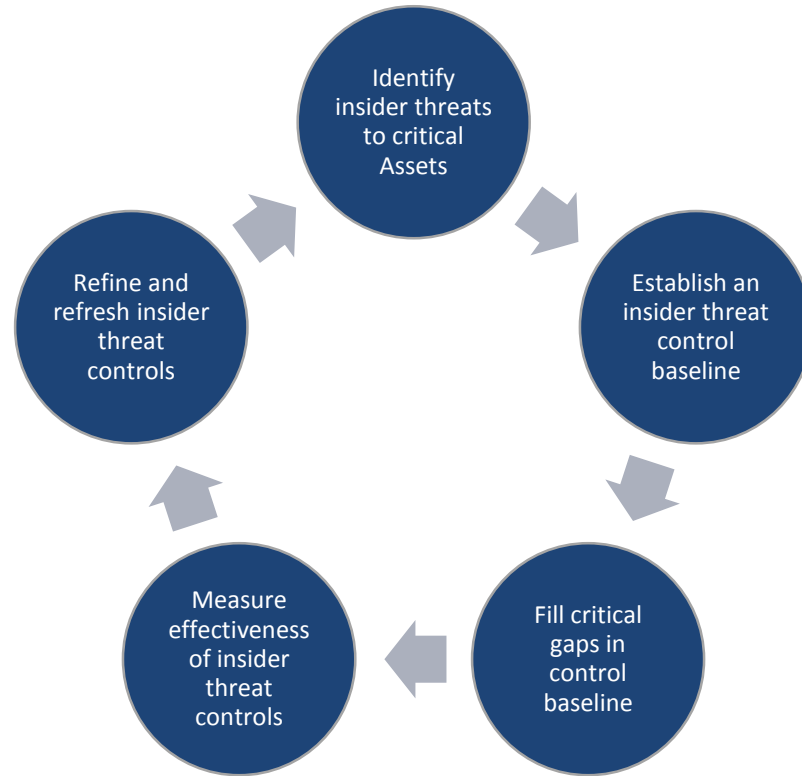
Overlap in functionality between tool types

- Fine line between defense-in-depth and buying the same thing twice

“Out of the box” functionality is a loaded concept

- Every organization’s priorities are different
- Every organization’s risk appetite is different
- Every organization’s ‘normal’ is different
- False positives for detective insider threat tools are potentially more damaging than externally-originating attacks

# A Use-Case Based Approach to Insider Threat Control Implementation and Operation







# Use-Case Based Data Source Prioritization Example

Use Case	Use Case Priority	Observable	HR System	DLP Logs	Help Desk Tickets	Active Directory Logs	Windows Event Logs
Departing Employee IP Theft	HIGH	Employee Termination	X				
	HIGH	Data Exfiltration		X			
Unauthorized Account Creation	MEDIUM	Account Creation				X	
	MEDIUM	Job Role of Account Creator	X				
	MEDIUM	No Associated Help Desk Ticket			X		
Clearing Security Logs	LOW	Windows Security Logs Cleared					X
...							
<b>Data Source Priority Score</b>			<b>5</b>	<b>3</b>	<b>2</b>	<b>2</b>	<b>1</b>

# Avoiding Vendor Lock-In

Ask yourself: where are the requirements and designs for your detective controls being documented?

- If the answer is 'in my UAM/SIEM/UBA tool', then changing tools will be a significant challenge

Consider a repository for controls where you document things like

- Detailed descriptions for the control
- Associated threat scenarios and / or indicators
- Revision history to the control
- Measures of effectiveness



# Specifying Control Requirements – 1

Control requirements can be conceptualized in a tool-agnostic way as a combination of the four following pieces of information for a given use case:

- The data source
- The specific fields within that data source
- The analytic techniques that are applied to the fields
- The response options, the actions taken when the control takes an action

Why bother?

- For the same reasons we bother with software architectures
- To make it easier for more stakeholders to participate in the control development and refinement process

<https://insights.sei.cmu.edu/insider-threat/2019/05/high-level-technique-for-insider-threat-programs-data-source-selection.html>

# Specifying Control Requirements – 2

Use Case	Data Source	Fields	Analytic Techniques	Response Options
Failed software installation attempt	Windows event logs – software installation	Event success/failure	Value match – failure	Generate an alert (low)
Interactive login of service account	Authentication server logs	Account associated with authentication event  Login type	Value match -interactive	Generate an alert (low or medium – Do service accounts typically login interactively within the organization?)
	Active directory logs	Account type (of account from the authentication server log)	Value match – service account	Enable enhanced monitoring
Successful unauthorized software installation attempt	Windows event logs – software installation	Event success/failure, software name	Value match – success; pattern match – software name not in a list of approved software	Generate an alert (high)  Enable enhanced monitoring

# Software Test Plans for InT Controls

## 1.1 Test 1 - Encrypted File Trigger

Generates an alert when an encrypted file is created, modified, or deleted.

### Prerequisites

- One Windows system under test with UAM agent deployed
- Permissions to create an encrypted file on the system under test
- The 7Zip tool

### Test Procedure

1. On the system under test, create an empty text file named "t1.txt" on the Desktop.
2. Encrypt the file created in step 1 using the 7Zip utility. Record the time on the system under test this action is performed.
3. Create a new folder on the Desktop named "test".
4. Copy the encrypted file created in step 2 to the folder created in step 3. Record the time on the system under test this action is performed.
5. Delete the file created in step 2. Record the time on the system under test this action is performed.
6. Move the file created in step 4 to the Desktop. Record the time on the system under test this action is performed.
7. Rename the file moved in step 6 to "t1.newextension". Record the time on the system under test this action is performed.

### Verification Points

Verify that alerts were generated that record the correct user, policy name, file name, file path, and time stamp for steps 2, 4, 5, 6, and 7.

## IEEE Standard 829 – Software Test Documentation

For each use case, document:

- The prerequisite activities needed for the test
- The test procedure – the specific actions to be taken
- Verification points – steps taken to confirm expected results
  - These should align with the prerequisites, test procedure steps, and the control's response options.

# Questions / Presenter Contact Information

Dan Costa, CISSP, PSEM

Technical Manager, CERT National Insider Threat Center

[dlcosta@sei.cmu.edu](mailto:dlcosta@sei.cmu.edu)

# Featured Research from the CERT National Insider Threat Center – 1

The Common Sense Guide to Mitigating Insider Threats, Sixth Edition – a collection of 21 best practices for insider threat mitigation, complete with case studies and statistics

- <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644>

Balancing Organizational Incentives to Counter Insider Threat – a study on how positive incentives can complement traditional security practices to provide a better balance for organizations' insider threat programs

- <https://ieeexplore.ieee.org/abstract/document/8424655>



# Featured Research from the CERT National Insider Threat Center – 2

Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump-Start an Insider Threat Program – an exploration of the types of tools that organizations can use to prevent, detect, and respond to multiples types of insider threats

- [https://resources.sei.cmu.edu/asset\\_files/WhitePaper/2018\\_019\\_001\\_521706.pdf](https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_521706.pdf)

Insider Threats Across Industry Sectors – a multi-part blog series that contains the most up-to-date statistics from our database on sector-specific insider threats

- <https://insights.sei.cmu.edu/insider-threat/2018/10/insider-threat-incident-analysis-by-sector-part-1-of-9.html>

# Featured Research from the CERT National Insider Threat Center – 3

## Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls

- <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=446367>

## Analytic Approaches to Detect Insider Threats

- <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=451065>

## Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments

- <https://web.archive.org/web/20170122065908/http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=48668>

# Featured Research from the CERT National Insider Threat Center – 4

## Workplace Violence & IT Sabotage: Two Sides of the Same Coin?

- [https://resources.sei.cmu.edu/asset\\_files/Presentation/2016\\_017\\_001\\_474306.pdf](https://resources.sei.cmu.edu/asset_files/Presentation/2016_017_001_474306.pdf)

## An Insider Threat Indicator Ontology

- <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=454613>

# Training from the CERT National Insider Threat Center

Our insider threat program manager, vulnerability assessor, and program evaluator certificate programs and insider threat analyst training courses are now available in live-online delivery formats!



For more information, please visit  
[www.sei.cmu.edu/education-outreach/courses/index.cfm](http://www.sei.cmu.edu/education-outreach/courses/index.cfm)