Current Trends in Insider Threat Detection Capability - What Does an Effective Program Look Like?

Randall Trzeciak
January 29, 2019
Notices

Copyright 2018 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.

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.


DM18-0089
Could This Happen to Your Organization?

Recently Demoted Software Engineer Steals Over $1B Worth Of Technology, Goes to Work for Foreign Competitor

Former Information Security Director at Lottery Association Uses Rootkit To Alter Random Number Generator, Allowing Accomplices to Win $14M

Disgruntled Contract Employee At Wastewater Facility Accesses SCADA Systems After Termination, Releases 800,000 Litres of Sewage
The CERT Insider Threat Center

Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber and physical threats

Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats
Insider Threat Mitigation

Insiders
- Not Alienate

Insider Threat
- Identify / Deter
- Consistent Response
  if detected

Insider Incident
- Prevent / Detect
- Respond / Recover
  if detected

Insider Threat Program
CERT’s Definition of Insider Threat

The potential for an individual who has or had authorized access to an organization’s assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.
What / Who is an Insider Threat?

Individuals

- Current or Former
- Full-Time Employees
- Part-Time Employees
- Temporary Employees
- Contractors
- Trusted Business Partners
What / Who is an Insider Threat?

Individuals
- Current or Former Employees
- Full-Time Employees
- Part-Time Employees
- Temporary Employees
- Contractors
- Trusted Business Partners

Organization’s Assets
- People
- Information
- Technology
- Facilities

Intentionally or Unintentionally
- Fraud
- Theft of Intellectual Property
- Cyber Sabotage
- Espionage
- Workplace Violence
- Social Engineering
- Accidental Disclosure
- Accidental Loss or Disposal of Equipment or Documents

Negatively Affect the Organization
- Harm to Organization’s Employees
- Degradation to CIA of Information or Information Systems
- Disruption of Organization’s Ability to Meet its Mission
- Damage to Organization’s Reputation
- Harm to Organization’s Customers
The Insider Threat

There is not one “type” of insider threat

- Threat is to an organization’s critical assets
  - People
  - Information
  - Technology
  - Facilities
- Based on the motive(s) of the insider
- Impact is to Confidentiality, Availability, Integrity

\[
\text{Cyber attack} = \text{Cyber Impact} \\
\text{Kinetic attack} = \text{Kinetic Impact} \\
\text{Cyber attack} = \text{Kinetic Impact} \\
\text{Kinetic attack} = \text{Cyber Impact}
\]
Insider Threat Observables

The CERT National Insider Threat Center has amassed a repository of over 2500 Insider incidents.

Potential Insider Threat Risk Indicators (not a complete list)
Types of Malicious Insider Incidents
TRUE STORY: IT Sabotage

911 services disrupted for 4 major cities

Disgruntled former employee arrested and convicted for this deliberate act of sabotage.
TRUE STORY: Theft of IP

Research scientist downloads 38,000 documents containing his company’s trade secrets before going to work for a competitor…

Information was valued at $400 Million.
TRUE STORY: Fraud

An undercover agent who claims to be on the “No Fly list” buys a fake drivers license from a ring of DMV employees...

The identity theft ring consisted of 7 employees who sold more than 200 fake licenses for more than $1 Million.
<table>
<thead>
<tr>
<th></th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current or former Employee?</strong></td>
<td>Former</td>
<td>Current</td>
<td>Current (within 30 days of resignation)</td>
</tr>
<tr>
<td><strong>Type of position</strong></td>
<td>Technical (e.g., sys admins, programmers, DBAs)</td>
<td>Non-technical (e.g., data entry, customer service) or their managers</td>
<td>Technical (e.g., scientists, programmers, engineers) or sales</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td>Male</td>
<td>Fairly equally split between male and female</td>
<td>Male</td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td>Network, systems, or data</td>
<td>PII or Customer Information</td>
<td>IP (trade secrets) or Customer Information</td>
</tr>
<tr>
<td><strong>Access Used</strong></td>
<td>Unauthorized</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>Outside normal working hours</td>
<td>During normal working hours</td>
<td>During normal working hours</td>
</tr>
<tr>
<td><strong>Where</strong></td>
<td>Remote access</td>
<td>At work</td>
<td>At Work</td>
</tr>
</tbody>
</table>
Unintentional (Non-Malicious) Insider Incidents

**UIT - Four Categories:**

**DISC** - accidental disclosure (e.g., via the Internet)
- sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail

**PHISHING/SOCIAL** - malicious code (UIT-HACKing, malware/spyware)
- an outsider’s electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) and carried out via software, such as malware and spyware

**PHYS** - improper/accidental disposal of physical records
- lost, discarded, or stolen non-electronic records, such as paper documents

**PORT** - portable equipment no longer in possession
- lost, discarded, or stolen data storage device, such as a laptop, PDA, smart phone, portable memory device, CD, hard drive, or data tape
Building an Insider Threat Program
Goal for an Insider Threat Program

Opportunities for prevention, detection, and response for an insider incident
Essential Elements of an Insider Threat Program

Insider Threat Program Roadmap

1. Initial Planning
2. Identify Stakeholders
3. Achieve & Sustain Leadership Buy-In
4. Risk Management Process
5. Detailed Project Planning
6. Develop Governance Structure and Policy
7. Communications, Training, and Awareness
8. Develop Detection Indicators
9. Data and Tool Requirements
10. Data Fusion
11. Analysis & Incident Management
11.1 Triage/Initial Evaluation
11.2 Internal Investigation
11.3 Refer/Report
11.4 External Criminal Investigation?
11.5 Final Action
12. Management Reporting
13. Feedback & Lessons Learned

Source: https://www.insaonline.org/insider-threat-roadmap/
CERT Insider Threat Center Key Components of an Insider Threat Program

- Integration with Enterprise Risk Management
- Insider Threat Practices Related to Trusted Business Partners
- Prevention, Detection, and Response Infrastructure
- Insider Threat Training and Awareness
- Data Collection and Analysis Tools, Techniques, and Practices
- Policies, Procedures and Practices to Support the InTP
- Protection of Employee Civil Liberties and Privacy Rights
- Communication of Insider Threat Events
- Insider Threat Incident Response Plan
- Confidential Reporting Procedures and Mechanisms
- Oversight of Program Compliance and Effectiveness
- Organization-wide Defined Program
- Formalized and Defined Program
- Oversight of Program Participation

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.
Tools to Support Insider Threat Mitigation
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 ...
Insider Threat Tools Vary in Features and Functions

- **Prevent**
  - Stop something from happening
  - Example: Block a sensitive document from being moved to removable media

- **Detect**
  - Figure out that something is happening (or about to happen)
  - Example: Alert security staff of (suspicious?) file activity

- **Deter**
  - Discourage something from happening
  - Example: Present a dialog that requires a user to acknowledge the organization’s removable media policy

- **Respond**
  - Address something that happened
  - Example: Restore missing data from backups

**Tools and Features**

- Auditing Host-based Activity
- Auditing Network-based Activity
- Preventing Data from Leaving Authorized Locations
- Data Visualization
- Rule-Based Alerting
- Anomaly Detection
- Data Correlation / Entity Resolution
- Risk Scoring
- Text Analysis
- Machine Learning
- Identity Management / Access Management

**Others**

- Case / Incident Management
- Data Masking / Anonymization
- ... And More ...
Anomaly Detection
Indicators

Technical
• Technical actions that could do your organization harm

Behavioral
• Common precursors to insider activity

Temporality and sequence
• 30-day rule

Context is key
• Stimulus
• Job role

Qualities of effective indicators
• Weighting
• Specificity
Behavioral Data
Behavioral Data Sources

Human Resources Management System Data
Help Desk Trouble Ticket System Logs
Physical Access Logs
Phone Logs
Personnel Security Systems
Foreign Travel and Reporting Systems
Financial Systems
Technical Data
Security Device Reporting Analysis

Operations analysts within the SOC typically monitor consoles where large amounts of information are collected from the security ‘sensors’ and devices.

This set of information includes

• IDS alerts
• IPS alerts
• Antivirus alerts
• Firewall logs
• Proxy logs
• Network flow records
• Packet capture and session recreation information
• Correlated events from security event managers
• External (global) threat and architecture information
# Tools for Detecting and Preventing Insider Incidents

## User Activity Monitoring (UAM)
- Observe and record host-based activities of individuals (applications executed, file access and modification, clipboard activity)
- Key capabilities: rule-based alerting, screen capture / video recording, analyst interface

## Data Loss Prevention (DLP)
- Detect and prevent sensitive information from leaving authorized locations
- Key capabilities: data tagging, content inspection, active monitoring of print jobs, removable media, file systems, and networks

## Security Information Event Management (SIEM)
- Log aggregation and analysis capability typically found in security operations centers (SOC’s)
- Key capabilities: data visualization, rule-based alerting, reporting, data normalization

## Analytics
- Broad range of tools that perform advanced analytics for insider threat prevention and detection
- Key capabilities: anomaly detection, risk scoring, predictive analytics, text analytics

## Forensics
- Tools that provide incident responders with detailed low-level views of user activity
- Key capabilities: storage medium acquisition, forensic artifact extraction, forensic artifact management and analysis
Hub Tools – UAM / UBA

User Activity Monitoring (UAM): “UAM refers to the technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing … information in order to detect insider threats and support authorized investigations.” –NITTF Guide

Often serves as the starting point and core of an insider threat analysis hub.

User Behavioral Analytics (UBA): “cybersecurity process about detection of insider threats, targeted attacks, and financial fraud. UBA solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns—anomalies that indicate potential threats. Instead of tracking devices or security events, UBA tracks a system's users.” - Gartner

https://www.gartner.com/doc/2831117-market-guide-user-behavior-analytics
Best Practices for the Mitigation of Insider Threats
### Recommended Best Practices for Insider Threat Mitigation

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

[http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738](http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738) or search “cert common sense guide insider threat”
CERT Publications and References


Moore, Andrew; Savinda, Jeff; Monaco, Elizabeth; Moyes, Jamie; Rousseau, Denise; Perl, Samuel; Cowley, Jennifer; Collins, Matthew; Cassidy, Tracy; VanHoudnos, Nathan; Buttles-Valdez, Palma; Bauer, Daniel; & Parshall, Allison. *The Critical Role of Positive Incentives for Reducing Insider Threats*. CMU/SEI-2016-TR-014. Software Engineering Institute, Carnegie Mellon University. 2016.

Many more at: https://www.cert.org/insider-threat/publications/index.cfm
Wrap Up
Point of Contact

Insider Threat Technical Manager
Randall F. Trzeciak
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-7040 – Phone
rft@cert.org – Email

http://www.cert.org/insider_threat/