Insider Threat Detection: Lessons from the Trenches Based on Real Insider Cases

Michael C. Theis, SAC (Retired), CISSP
Assistant Director for Research, CERT Insider Threat Center
Software Engineering Institute, Carnegie Mellon University

iSMG INFORMATION SECURITY MEDIA GROUP

FRAUD & BREACH PREVENTION SUMMIT

Copyright 2017 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

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.

This material has been approved for public release and unlimited distribution except as restricted below.

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.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0002495

About the Speaker

Michael C. Theis, *SAC (retired), CISSP*

Assistant Director for Research,
CERT Insider Threat Center

Theis heads a team focusing on insider threat research; threat analysis; modeling; assessments; and training. He has over 25 years of experience as a supervisory special agent in counterintelligence; and over 30 years in IT systems engineering and security; he leverages both of these skill areas in his role to help the CERT Insider Threat Center develop and transition socio-technical controls for the prevention, detection, and response to malicious and unintentional insider threats.

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 threats*

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

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

Cyber attack = Cyber Impact

Kinetic attack = Kinetic Impact

Cyber attack = Kinetic Impact

Kinetic attack = Cyber Impact

What / Who is an Insider Threat?

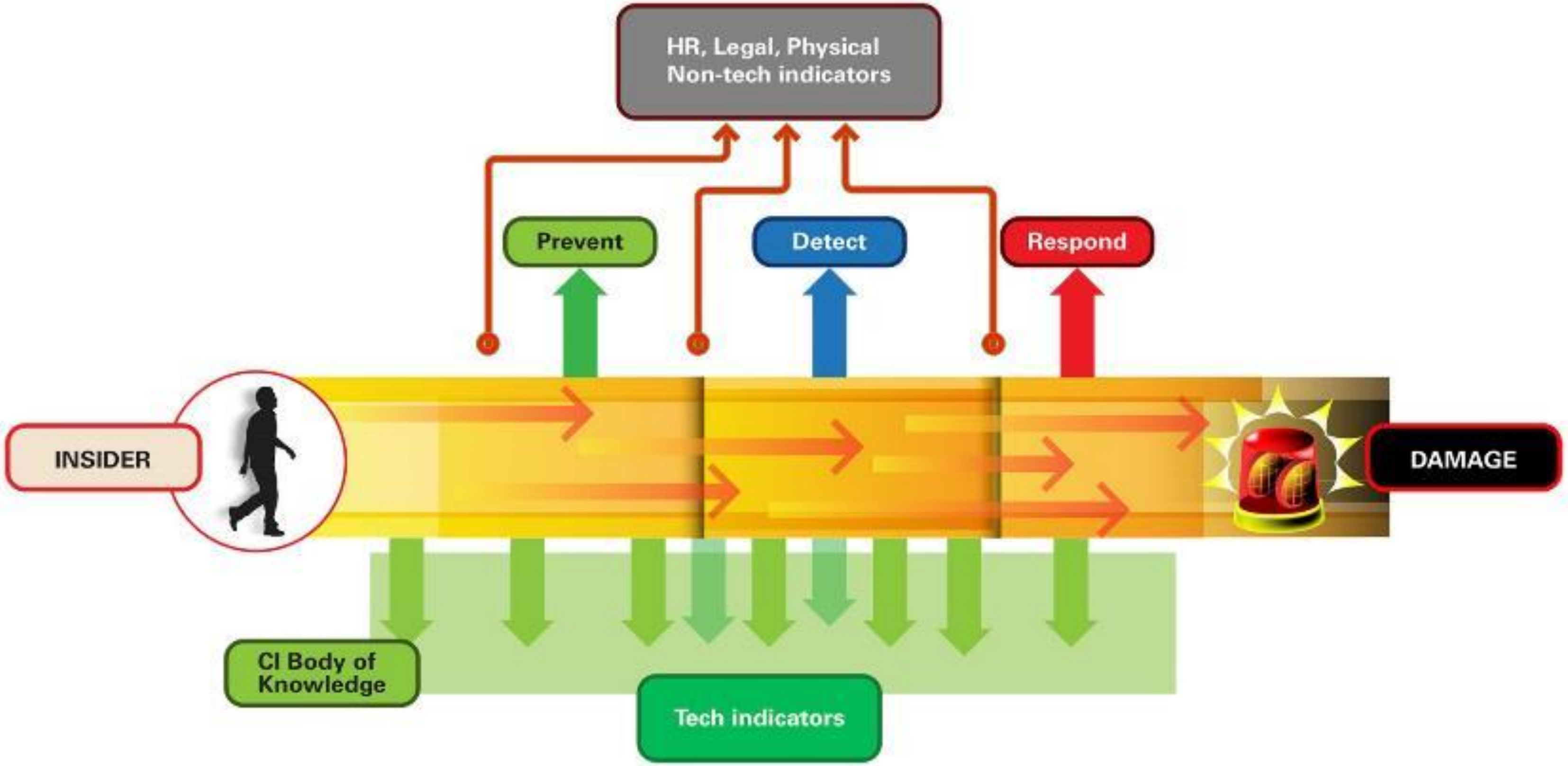
The ***potential*** for an individual who has or had authorized access to an organization's *assets* to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

What / Who is an Insider Threat?

Individuals

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

Goal for an Insider Threat Program



Opportunities for prevention, detection, and response for an insider incident

Types of Malicious Insider Incidents

Types of Insider Activities - 1

Insider IT Sabotage

An insider’s use of IT to direct specific harm at an organization or an individual

- Deletion of information
- Bringing down systems
- Website defacement to embarrass organization

Insider Theft of Intellectual Property

An insider’s use of IT to steal intellectual property from the organization

- Proprietary engineering designs, scientific formulas, etc.
- Proprietary source code
- Confidential customer information
- Industrial Espionage and Trade Secrets

Types of Insider Activities - 2

Insider Fraud

An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud

- Payroll
- Reimbursement
- Unauthorized acquisitions

Theft and sale of confidential information

- SSN, PII, etc.
- Credit card numbers

Modification of critical data for a fee

- Driver's license records
- Criminal records
- Qualification for welfare, etc.

Unintentional Insider Threat (UIT)

An insider whose actions or lack of action without malicious intent causes harm or the possibility of harm

Types of Insider Activities - 3

Insider National Security Espionage

- – The act of communicating, delivering or transmitting information pertaining to the national defense of the United States to any foreign government or faction, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation
  - Volunteers
  - Recruited in Place
  - Dispatched

Insider Miscellaneous

- – Unauthorized disclosure (information insider believed should be in the public domain)
- – Providing address of a person to an acquaintance who physically harmed the individual
- – Accessing records of high-profile individuals

Types of Insider Activities - 4

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

Insider Sabotage Example (Canada)

An Arts Education Organization in Canada under cyber-attack for over a year

Former employee (who was laid-off) used remote access to attack the former employer in this deliberate act of sabotage.

Other Cases of IT Sabotage

Financial Institution customers lose all access to their money from Friday night through Monday

- Fired system administrator sabotages systems on his way out

A logic bomb sits undetected for 6 months before finally wreaking havoc on a telecommunications firm

A security guard at a U.S. hospital, after submitting resignation notice, obtained physical access to computer rooms

- Installed malicious code on hospital computers, accessed patient medical records

SCADA systems for an oil-exploration company is temporarily disabled

- A contractor, who's request for permanent employment was rejected, planted malicious code following termination

System administrator at a manufacturing plant, passed over for promotion, deployed "logic bomb" prior to resigning, deleting critical software required to run operations

- Financial damage $10M; Forced to lay off 80 employees

Insider Theft of Intellectual Property (Canada)

Low ranking military official steals classified information, as well as IP and PII from protected databases in exchange for money

Insider had a history of bankruptcy and divorce, was single parent of multiple children. After initial thefts, was coerced by a foreign government to continue thefts

Other Cases of Theft of IP

Simulation software for the reactor control room in a US nuclear power plant was being run from outside the US…

- A former software engineer born in that country took it with him when he left the company.

Insider Fraud Example (Canada)

Insider was assistant manager of support services at a financial institution.

Made 60 transactions from the organization’s funds to their personal account, totaling over *$537,000.*

The insider had a *gambling problem.* The insider was arrested, convicted, ordered to forfeit all of the stolen money, and sentenced to 2 years imprisonment.

Other Cases of Fraud

An office manager for a trucking firm fraudulently puts her husband on the payroll for weekly payouts, and erases records of payments…

- Over almost a year loss of over $100K

A front desk office coordinator stole PII from hospital...

- Over 1100 victims and over $2.8 M in fraudulent claims

A database administrator at major US Insurance Co. downloaded 60,000 employee records onto removable and solicited bids for sale over the Internet

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.*

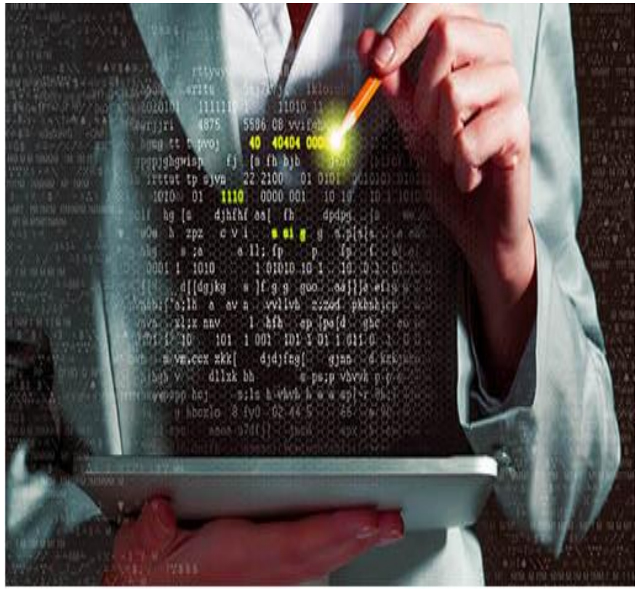
Summary of Insider Incidents

	IT Sabotage	Fraud	Theft of Intellectual Property
Current or former Employee?	Former	Current	Current (within 30 days of resignation)
Type of position	Technical (e.g., sys admins, programmers, DBAs)	Non-technical (e.g., data entry, customer service) or their managers	Technical (e.g., scientists, programmers, engineers) or sales
Gender	Male	Fairly equally split between male and female	Male
Target	Network, systems, or data	PII or Customer Information	IP (trade secrets) or Customer Information
Access Used	Unauthorized	Authorized	Authorized
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At Work

Insider Threat Detection

Observables

Insider Motives Observed in Cases



Financial Gain

Ideology

Revenge

Recognition

Curiosity

Excitement

Benefit a Foreign Entity

Gain a Competitive Business Advantage

Start a New Business

Benefit a New Employer

Unmet Expectations Observed in Cases

Salary/bonus

Promotion

Freedom of online actions

Workload

Overestimated abilities

Supervisor demands

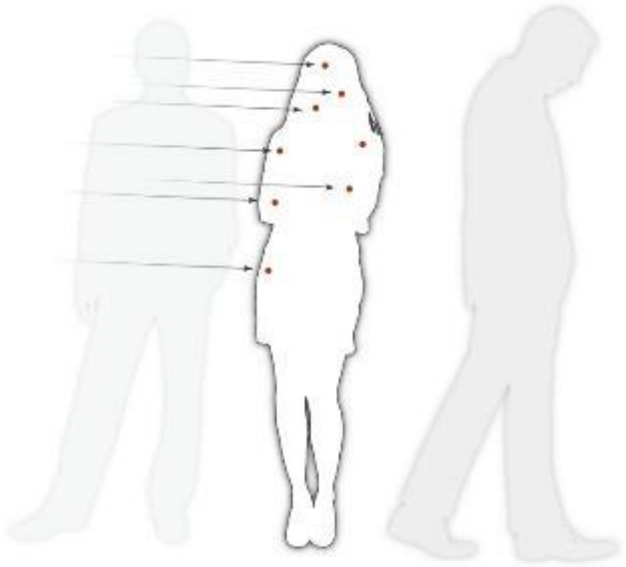
Coworker relations

Job engagement

Perceived organizational support

Connectedness at work

Behavioral Precursors Observed in Cases



Drug use

Conflicts (coworkers, supervisor)

Aggressive or violent behavior

Mood swings

Using organization’s computers for personal business

Poor performance

Absence/tardiness

Sexual harassment

Unknown Access Paths Observed in Cases

Planted logic bomb while still employed

Created backdoors before termination or after being notified of termination

Installed modem for access following termination

Changed all passwords right before resignation

Disabled anti-virus on desktop & tested virus

Network probing

Installed remote network administration tool

Downloaded and installed malicious code and tools (e.g., password cracker or virus)

Disabled system logs & removed history files

Technical Precursors Observed in Cases

Downloading and using tools such as rootkits, password sniffers, or password crackers

Disabling automated backups

Disabling logging / deleting log files

Failure to document systems or software as required

Unauthorized access of customers’ systems

Unauthorized use of coworkers’ machines left logged in

Sharing passwords with others & demanding passwords from subordinates

System access following termination

Network probing / data hoarding

Failing to swipe badge to record physical access

Access of web sites prohibited by acceptable use policy

Failure to return IT equipment upon termination

Creation and use of backdoor accounts

Mitigation Strategies

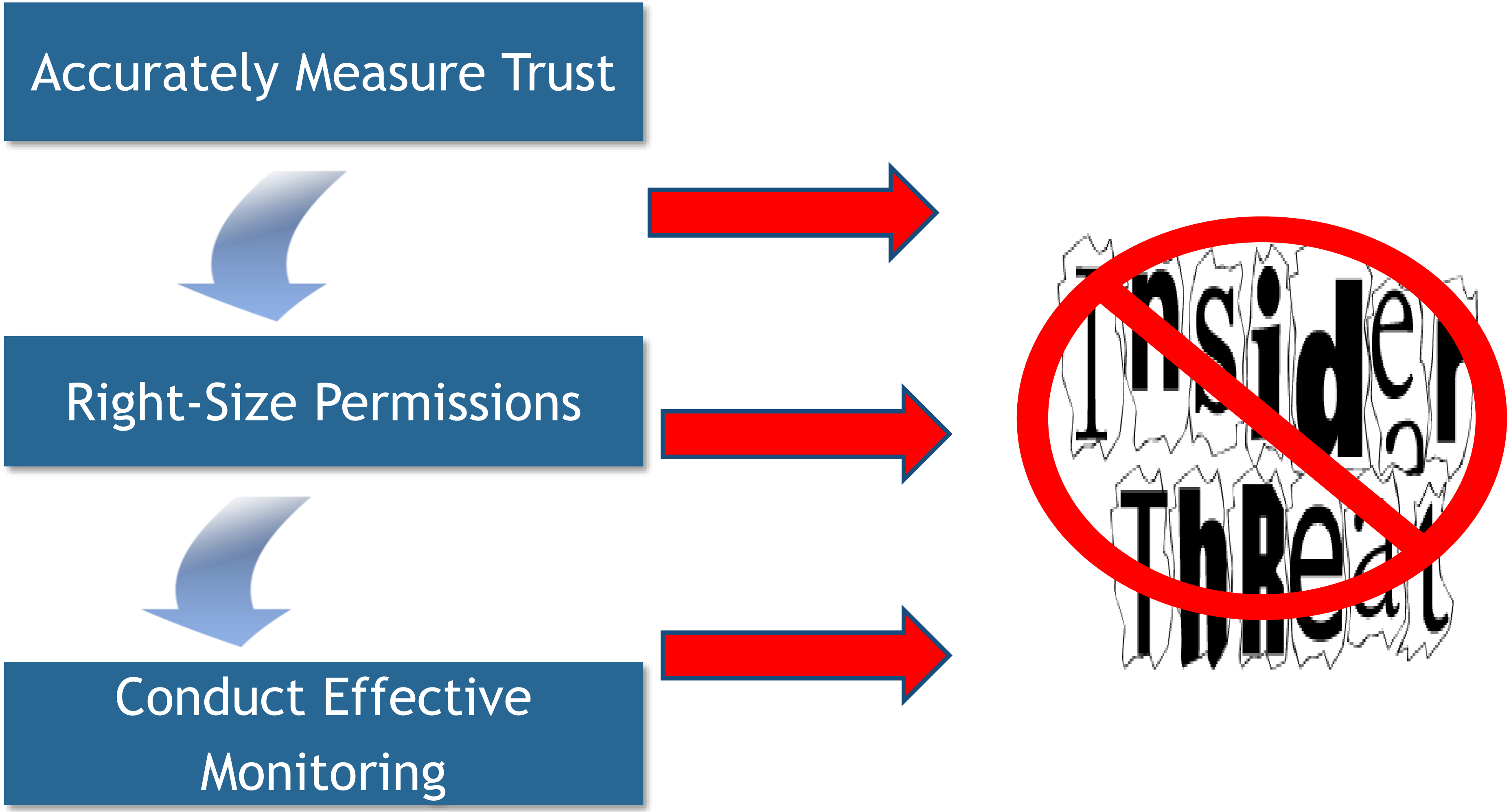
CERT Recommended Best Practices for Insider Threat Mitigation

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

CERT's Common Sense Guide to Mitigating Insider Threats, Fifth Edition

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738

The Three Pillars of a Robust Strategy



Accurately Measure Trust

Right-Size Permissions

Conduct Effective Monitoring

CERT’s Insider Threat Services

CERT Insider Threat Center Services

Building an Insider Threat Program

- Insider Threat Program Manager Certificate (ITPM-C)

Insider Threat Vulnerability Assessment

- Insider Threat Vulnerability Assessor Certificate (ITVA-C)

Evaluating an Insider Threat Program

- Insider Threat Program Evaluator Certificate (ITPE-C)

Insider Threat Control/Indicator Development / Deployment

Insider Threat Data Analytics Hub Development / Deployment

Insider Threat Training (1/2 day, 1 day, and 2 day interactive workshops)

Customized Insider Threat Research

- Ontology Development and Maintenance
- Sentiment / Linguistic Analysis
- Insider Threat Tool Evaluation Criteria Development

For More Information

Insider Threat Center website

http://www.cert.org/insider-threat/

Insider Threat Center Email:

insider-threat-feedback@cert.org

Insider Threat Blog

http://www.cert.org/blogs/insider-threat/

Point of Contact

Michael C. Theis, SAC (retired), CISSP
Assistant Director for Research
CERT Insider Threat Center

mctheis@cert.org

Software Engineering Institute (an FFRDC)
Carnegie Mellon University

4500 Fifth Avenue
Pittsburgh, PA 15213-3890

http://www.cert.org/insider-threat/

Questions

Thank you for attending!

Submit your feedback via the **ISMG Events** app.

Download on the App Store

GET IT ON Google Play

ISMG INFORMATION SECURITY MEDIA GROUP