Insider Threats: Practical Methods for Analysis and Detection

Randall Trzeciak (rft@cert.org)

August 7, 2018

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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 Incident Corpus

- Database of over 2000 insider threat incidents
  - Includes interviews of actual offenders
- Coded to allow analysis of technical actions & behaviors observables
- Development of technical controls to baseline and detect anomalous actions
- Research into areas of
  - Sentiment analysis
  - Workplace violence
  - Typing heuristics
  - Biometrics
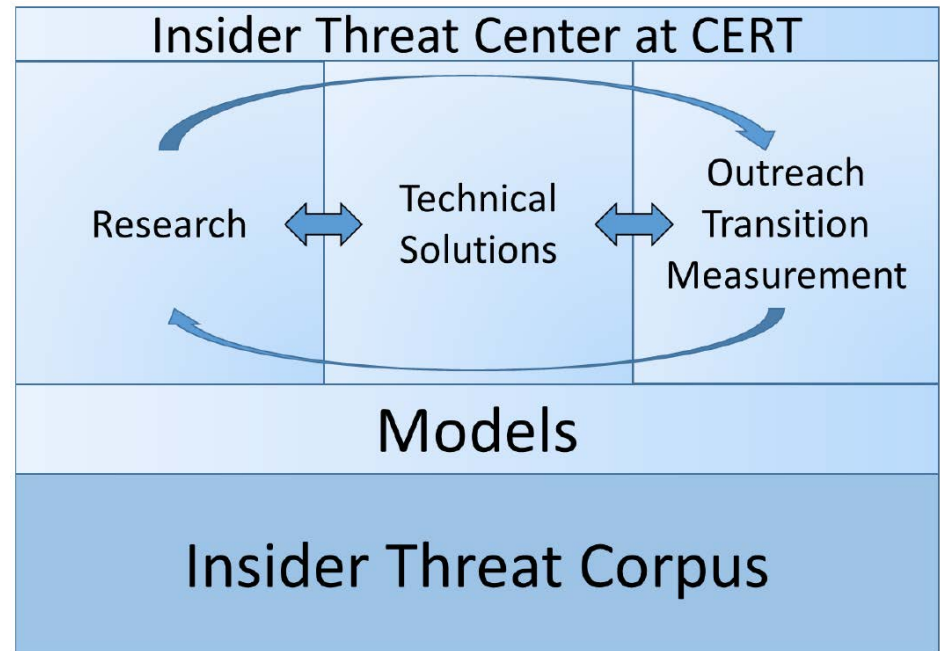
CERT Insider Threat Center Methodology

Collect, code, and empirically analyze incidents

Develop Causal Models
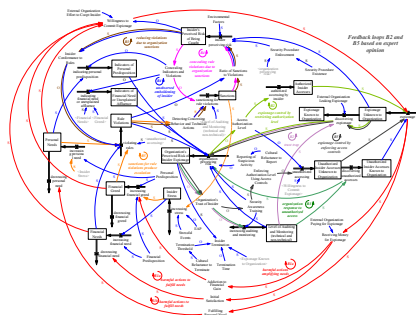
Deriving Candidate Controls and Indicators
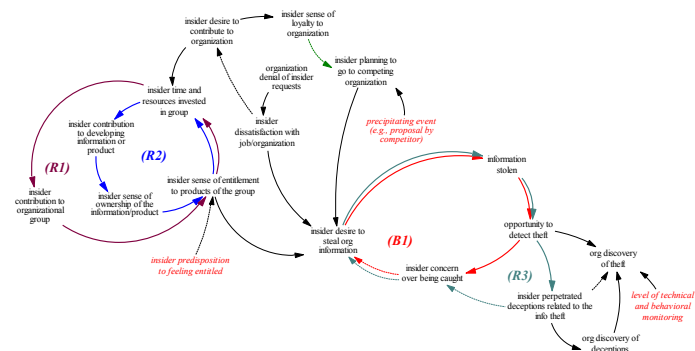
Our lab transforms that into this…

Splunk Query Name: Last 30 Days - Possible Theft of IP

Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was disabled. *" | eval
Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name "@corp.merit.lab"
sender_address | fields - Account_Name] total_bytes > 50000 AND recipient_address!="*corp.merit.lab"
startdaysago=30 | fields client_ip, sender_address, recipient_address, message_subject, total_bytes'

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

Software Engineering Institute | Carnegie Mellon University

What / Who is an Insider Threat?

Individuals

who have or had authorized access to

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

Organization's Assets

use that access

- People
- Information
- Technology
- Facilities

Intentionally or Unintentionally

to act in a way that could

- 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

Cyber attack = Cyber Impact

Kinetic attack = Kinetic Impact

Cyber attack = Kinetic Impact

Kinetic attack = Cyber Impact

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.

Insider Incidents in Tax Organizations-1

A clerk at a government entity exceeded their authorized access to the organization's database to investigate the parent of their grandchild. The insider, without any need-to-know, accessed the individual's account on 4 occasions. A government audit detected the incident. The insider was arrested and convicted.

An insider working for a government entity committed an act of Theft of IP by stealing customer PII in order to fill out fraudulent tax returns. The insider filled out more than 120 fraudulent forms and received about $300,000 from the tax returns. It is suspected that the insider had been accessing customer information and filing out the fraudulent tax returns for over 3 years.

Insider Incidents in Tax Organizations-2

An insider was employed by a state agency for 7 years and had access to customer information including customer names, addresses, dates of birth, and Social Security Numbers (SSNs). The insider would obtain the information and format it into a sheet then email to other outsiders. The outsiders would use the stolen PII to file fraudulent tax returns and would pay the insider to steal more customer information.

The insider stole PII of more than 3,000 customers, mostly those of teenagers.

The outsiders used all of the PII and filed federal income tax returns that claimed over $7.5 million in fraudulent refunds.

The insider plead guilty and was sentenced to more than 80 months imprisonment, 3 years supervised release, and over $3,000,000 ($3 Million) in restitution.

Insider Incidents in Tax Organizations-3

The insider was a current, full-time tax examiner for a government agency. The insider targeted Social Security Numbers (SSNs), which they had authorized access to, for the purposes of committing tax fraud.

The SSNs were obtained on-site and during work hours, whereas the fraudulent tax returns were filed outside of work hours.

The insider created multiple bank accounts and postal service boxes to receive funds from fraudulent tax returns and tax forms.

The insider pleaded guilty to 1 count Wire Fraud and 1 count Aggravated Identity Theft.

The insider was sentenced to 24 months and one day in prison followed by three years of supervised release. The insider was ordered to pay over $100,000 in restitution.

Insider Incidents in Tax Organizations-4

The insider worked as an auditor for the victim organization.

As part of their job they were responsible for conducting audits of client companies.

The insider was assigned to conduct an audit for a client company, however, they did not complete the audit as assigned. Instead the insider falsified official records to incorrectly show that they had completed the audit. In doing so the insider falsely signed off on the record as if they were the president of the client company.

The insider also falsified a form that stated this same client company needed an extension without authorization. The insider also falsified a form that appeared to be the approval from the client company consenting to this additional audit and the fees associated with it.

Insider Incidents in Tax Organizations-5

The insider was employed as a tax preparer by a tax preparation services organization.

While on site and during work hours, the insider printed personally identifiable information (PII) for at least 30 customers. The insider used this information to submit fraudulent tax returns with false aliases and the correct social security numbers (SSNs).

The refunds, totaling $290,000, were deposited into 17 bank accounts.

The incident was detected when the insider and their accomplice, an outsider, were pulled over under suspicion of driving under the influence. The officer noticed a credit card by her feet and subsequently performed a search of the insider, the accomplice, and the vehicle.

In the car, officers discovered blank W-2 forms, over 100 debit cards, and papers containing SSNs, PIN numbers, dates of tax return filings and whether the returns had been accepted.

Insider Incidents in Tax Organizations-6

The insider was employed at a state tax institution for 9 years, eventually becoming a supervisor.

The insider, their partner (C1), and their partner's spouse (C2) were involved in fraud against the state tax institution.

The insider would issue unclaimed tax credits to C1 and then deposit the refund in an account controlled by C1 or C2.

The insider was able to get around controls because the insider knew the user information of two of their former employees (whose accounts had not been deactivated).

The insider also helped to develop one of the systems which they used in the theft. The insider and their conspirators stole money in this way for almost two years.

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 Fraud: A Closer Look

Insider Fraud Study

Funded by U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T)

Conducted by the CERT Insider Threat Center in collaboration with the U.S. Secret Service (USSS)

Full report: "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector"
(http://www.sei.cmu.edu/library/abstracts/reports/12sr004.cfm)

Booklet: "Insider Fraud in Financial Services"
(http://www.sei.cmu.edu/library/abstracts/brochures/12sr004-brochure.cfm)

INSIDER FRAUD IN FINANCIAL SERVICES

Low and Slow

Criminals who executed a "low and slow" approach accomplished more damage and escaped detection for longer.
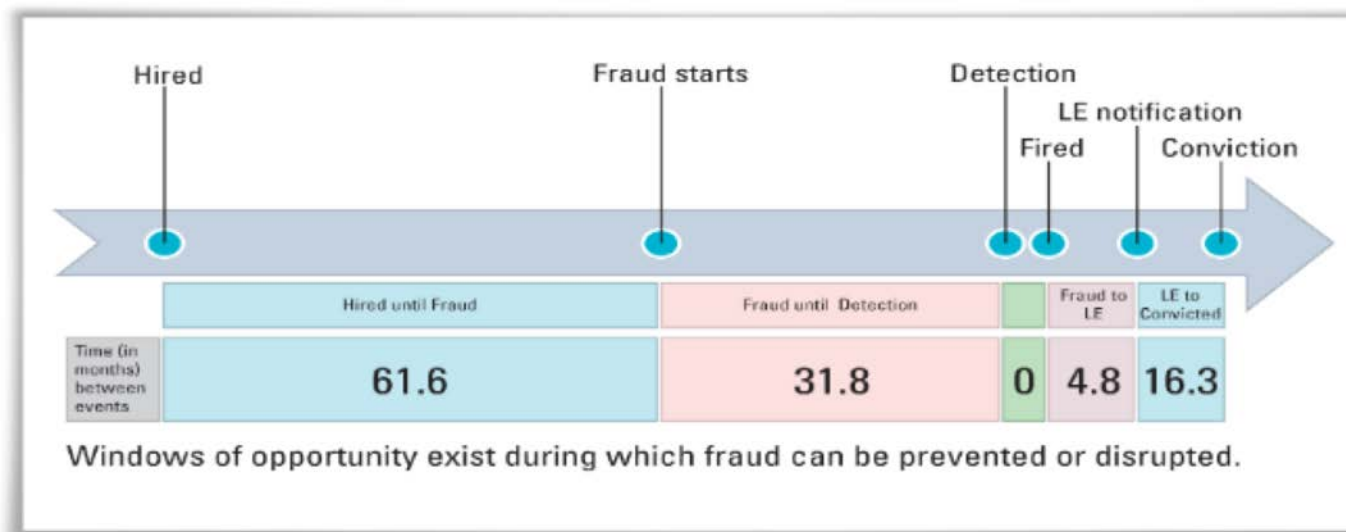
There are, on average, over 5 years between a subject's hiring and the start of the fraud. There are 32 months between the beginning of the fraud and its detection.

Low-Tech

Insiders' means were not very technically sophisticated.
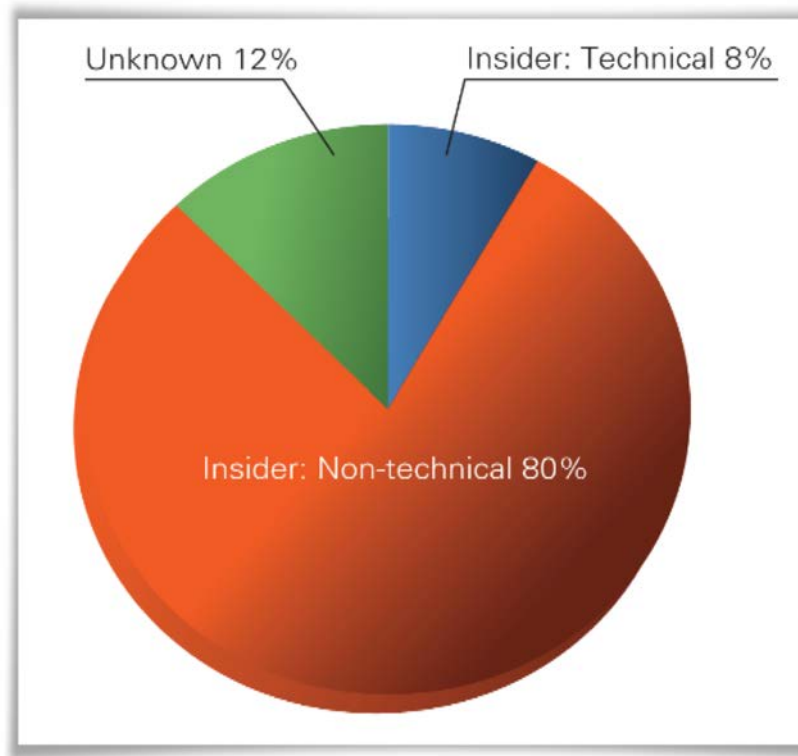
Non-technical subjects were responsible for 65 (81 percent) incidents. Seven were external attackers, but their methods were also non-technical.

CERT | Software Engineering Institute | Carnegie Mellon University

Managers vs. Non-Managers

Fraud by managers differs substantially from fraud by non-managers by damage and duration.
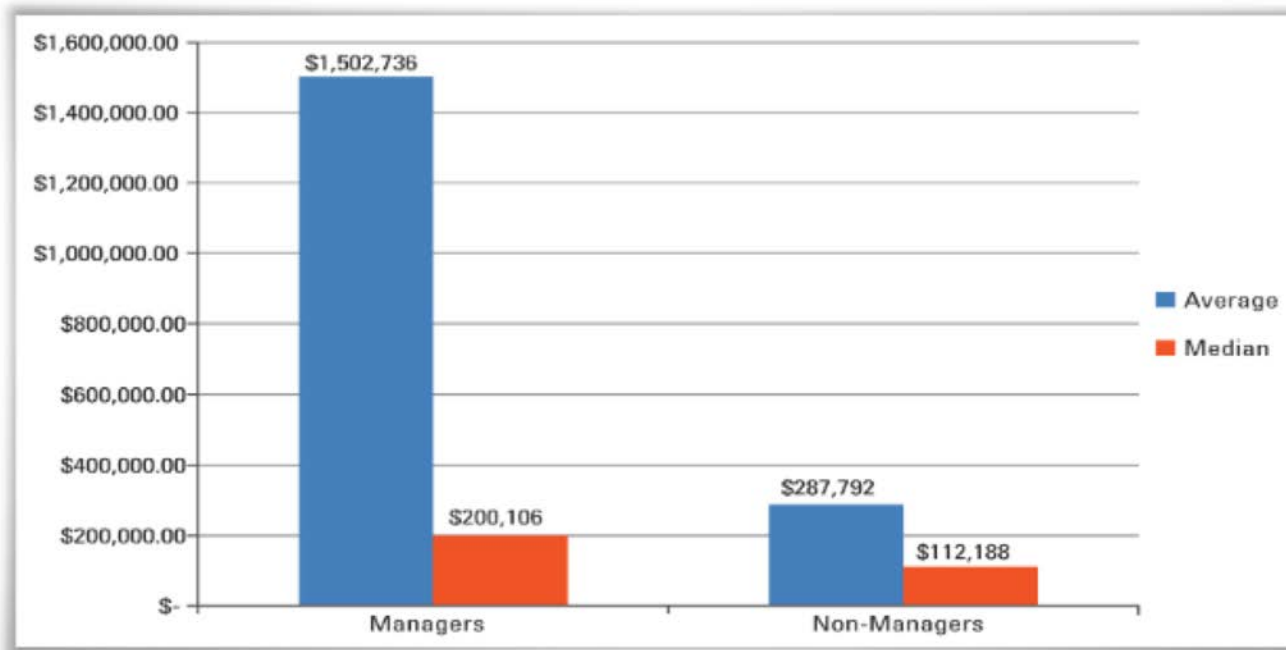
Of 61 subjects, 31 (51 percent) were managers, VPs, bank officers, or supervisors. The median results show that managers consistently caused more actual damage ($200,106) than non-managers ($112,188).

Collusion

Most cases do not involve collusion.

Cases by type of Collusion
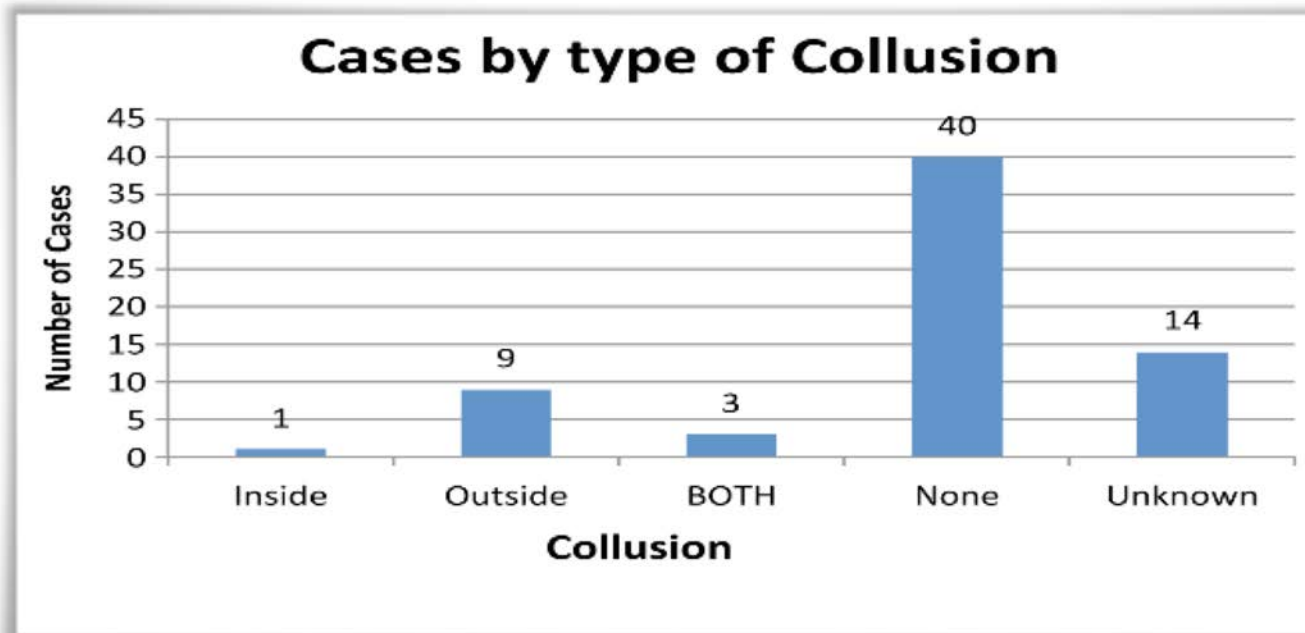
There was not a significant number of cases involving collusion, but those that did occur generally involved external collusion (i.e., a bank insider colluding with an external party to facilitate the crime).

Audits, Complaints, and Suspicions

Most incidents were detected through an audit, customer complaints, or co-worker suspicions.

The most common way attacks were detected was through routine or impromptu audits.

Over half of the insiders were detected by other victim organization employees, though none of the employees were members of the IT staff.

As expected, most initial responders to the incidents were managers or internal investigators (75 percent).

Building an Insider Threat Program

Goal for an Insider Threat Program
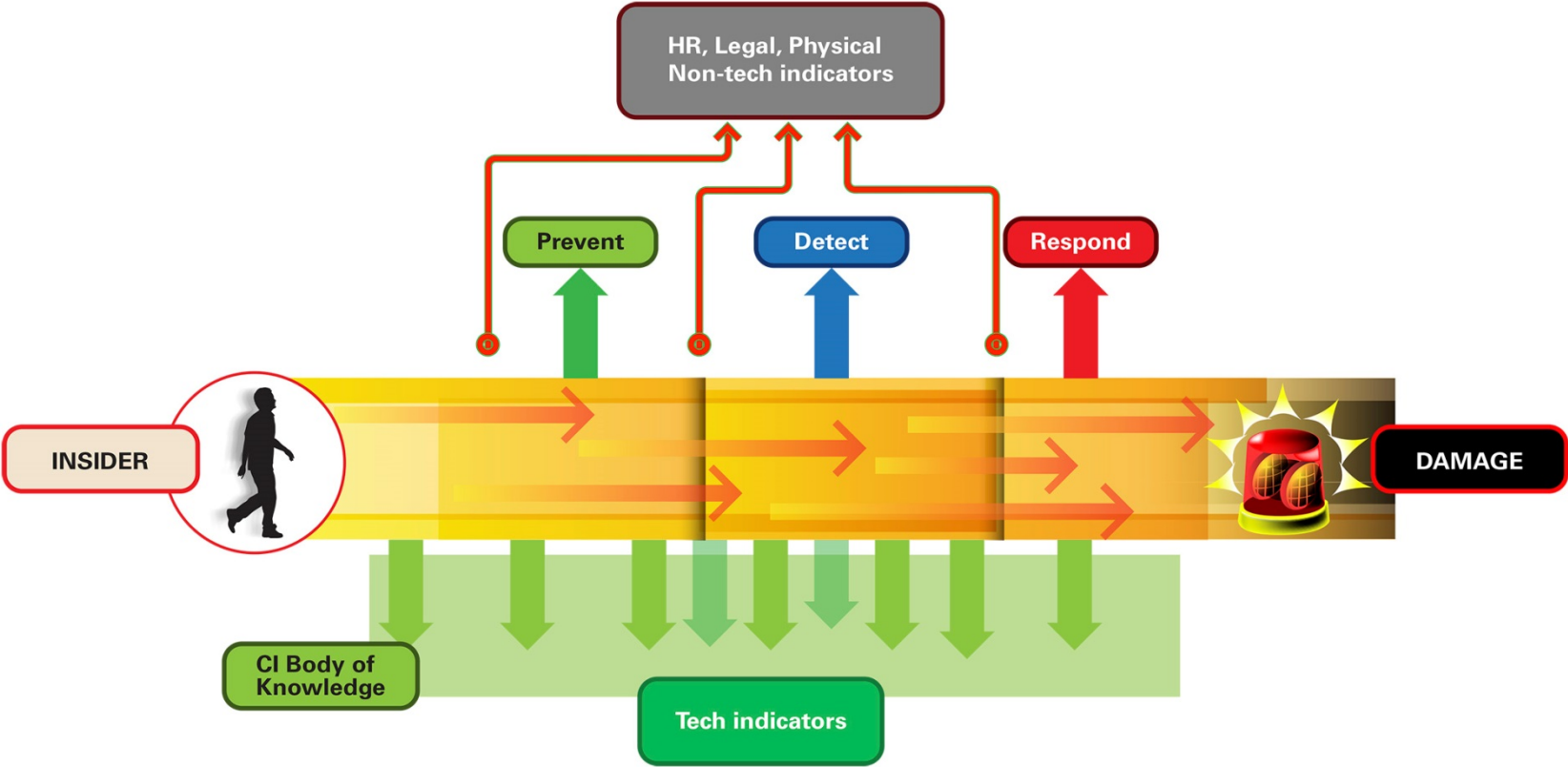
Opportunities for prevention, detection, and response for an insider incident

Essential Elements of an Insider Threat Program

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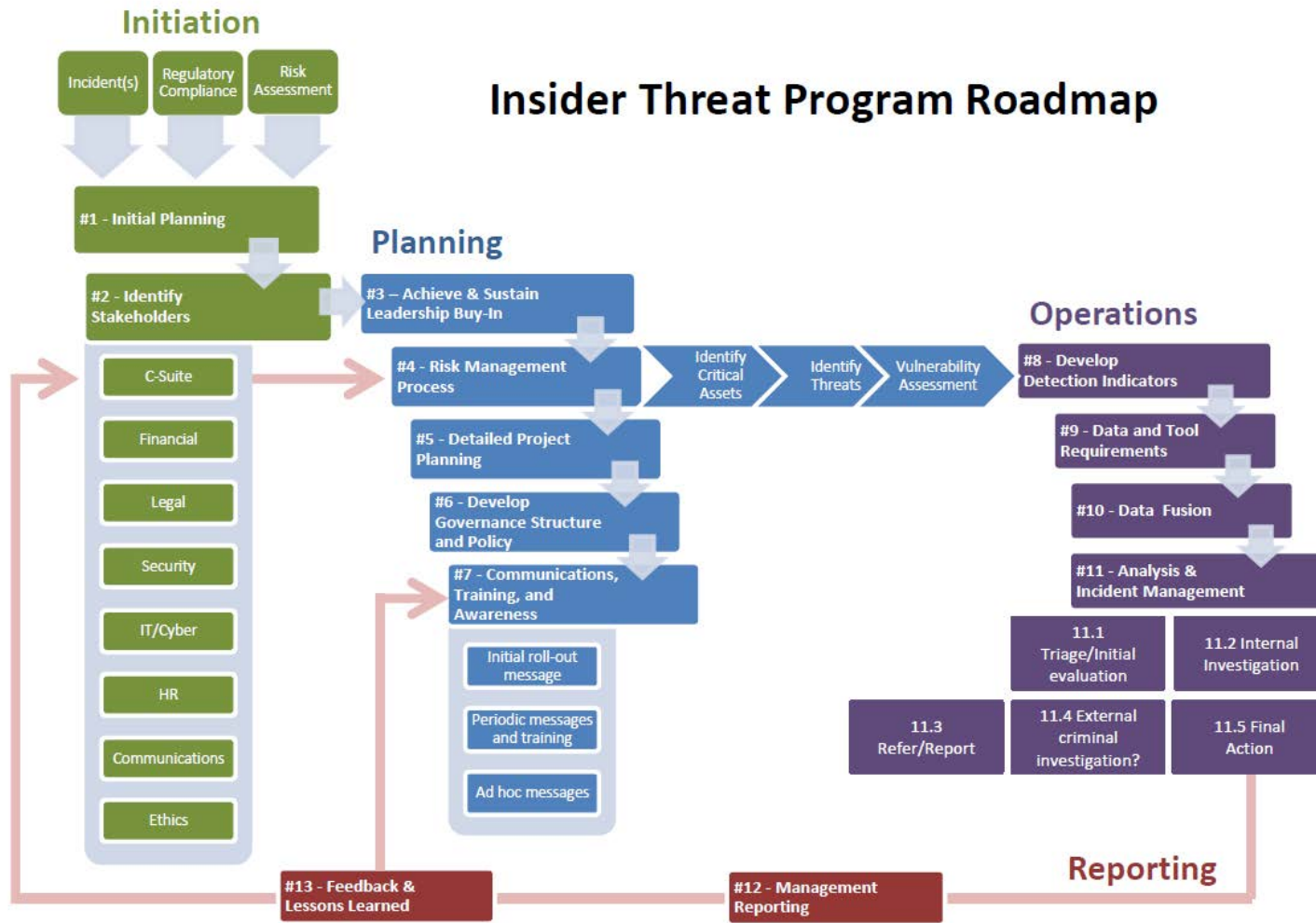
CERT Insider Threat Center Key Components of an Insider Threat Program

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 Participation

Formalized and Defined Program

Software Engineering Institute | Carnegie Mellon University

Observables
(Potential Indicators?)

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
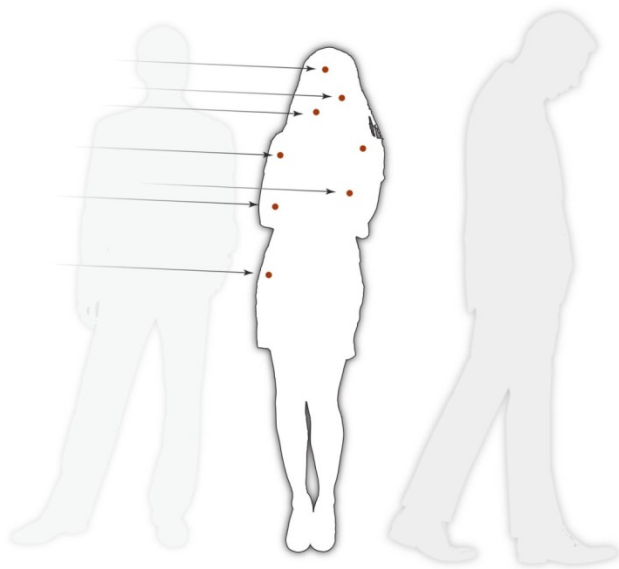
Unknown Access Paths Observed in Cases

- 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

Anomaly Detection

A Phased Approach to Insider Threat Anomaly Detection

Known Issues
- Policy Violations
- Sensitive Data Exfiltration
- Unauthorized Configuration Changes

Suspicious Events
- Unusual Patterns
- Unknown Error
- Unrecognized Events

Normal Activity
- Authorized Activities
- Scheduled Hardware Outages
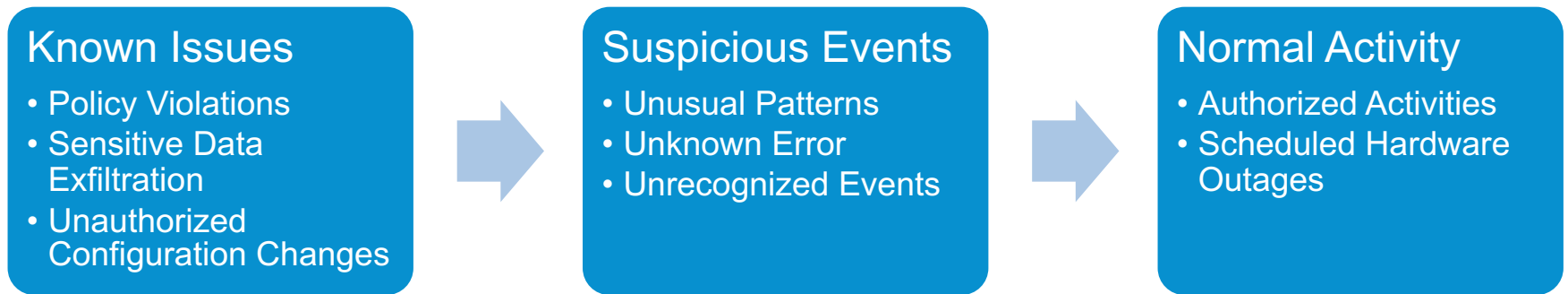
Baselining

Establish "normal behavior" across bins.

- User-Based
  - Compare each user to himself or herself.

- Role-Based
  - Compare users in the same roles against each other.

- Pattern-Based
  - Compare common patterns to previous occurrences of the pattern.

- Threshold-Based
  - Compare the average number of activities/events.

Indicator Development

Software Engineering Institute | Carnegie Mellon University

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

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

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

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

Best Practices for the Mitigation of Insider Threats

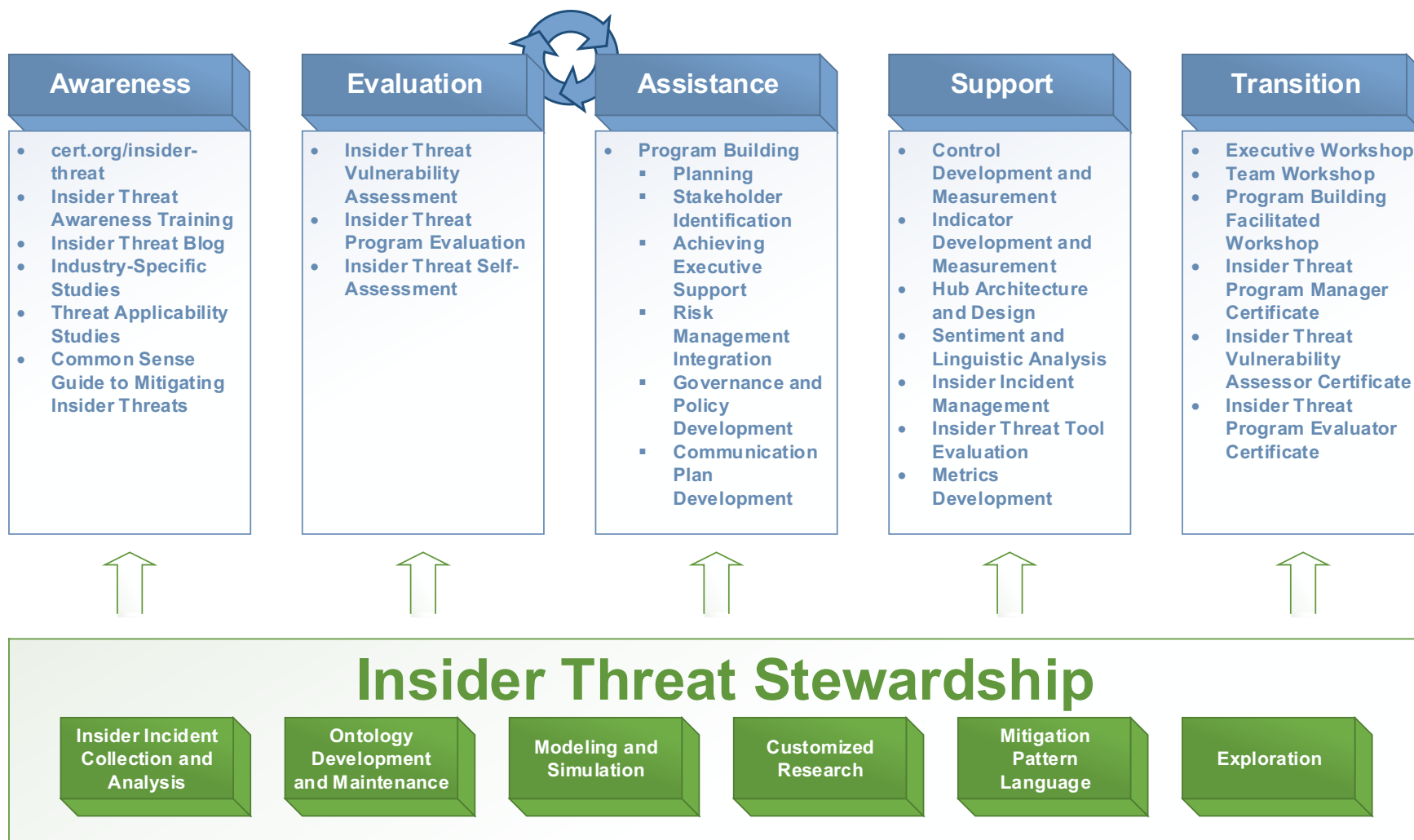# Recommended Best Practices for Insider Threat Mitigation

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.

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738 or search "cert common sense guide insider threat"

Wrap Up

Our Insider Threat Portfolio

Awareness
- cert.org/insider-threat
- Insider Threat Awareness Training
- Insider Threat Blog
- Industry-Specific Studies
- Threat Applicability Studies
- Common Sense Guide to Mitigating Insider Threats

Evaluation
- Insider Threat Vulnerability Assessment
- Insider Threat Program Evaluation
- Insider Threat Self-Assessment

Assistance
- Program Building
  - Planning
  - Stakeholder Identification
  - Achieving Executive Support
  - Risk Management Integration
  - Governance and Policy Development
  - Communication Plan Development

Support
- Control Development and Measurement
- Indicator Development and Measurement
- Hub Architecture and Design
- Sentiment and Linguistic Analysis
- Insider Incident Management
- Insider Threat Tool Evaluation
- Metrics Development

Transition
- Executive Workshop
- Team Workshop
- Program Building Facilitated Workshop
- Insider Threat Program Manager Certificate
- Insider Threat Vulnerability Assessor Certificate
- Insider Threat Program Evaluator Certificate

Insider Threat Stewardship

- Insider Incident Collection and Analysis
- Ontology Development and Maintenance
- Modeling and Simulation
- Customized Research
- Mitigation Pattern Language
- Exploration

Other 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 Analyst Training Course

- Insider Threat Control/Indicator Development / Deployment
- Insider Threat Data Analytics Hub Development / Deployment
- 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

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/