RSACONFERENCE2010

SECURITY DECODED

# The Key to Successful Monitoring for Detection of Insider Attacks

Dawn M. Cappelli
Randall F. Trzeciak
Robert Floodeen

Software Engineering Institute
CERT Program

Session ID: GRC-302
Session Classification: Intermediate

## 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.**

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

# Agenda

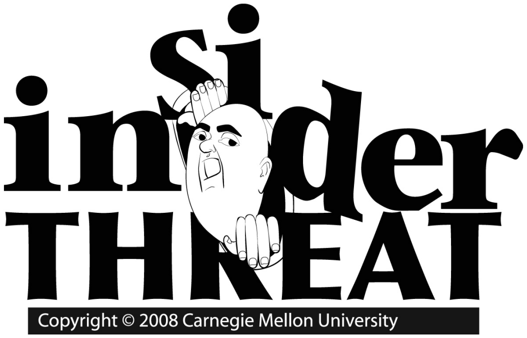
Insider Threat Center at CERT

IT Sabotage

Fraud / Theft of Information

Final Thoughts

# Insider Threat Center at CERT



# What is CERT?

- Center of Internet security expertise
- Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today
- Located in the Software Engineering Institute (SEI)
  - Federally Funded Research & Development Center (FFRDC)
  - Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

# CERT Insider Threat Center—Mission

Assist organizations in identifying indications and warnings of insider threat by

- performing vulnerability assessments
- assisting in the design and implementation of policies, practices, and technical solutions

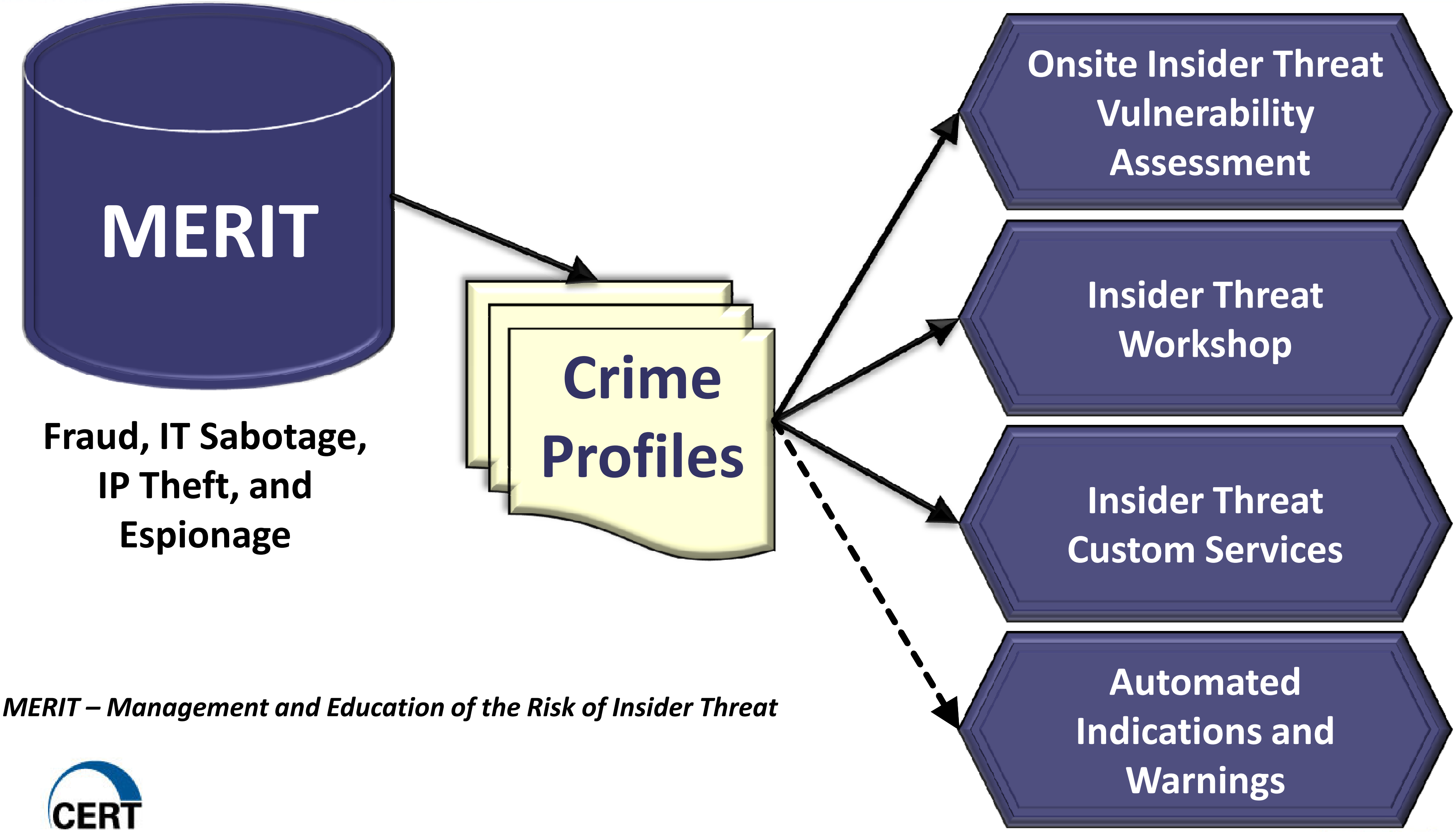
*based on our ongoing research of hundreds of actual cases of insider IT sabotage, theft of intellectual property, fraud, and espionage*

# Who is a Malicious Insider?

*Current or former employee, contractor, or other business partner who*

- *has or had authorized access to an organization’s network, system or data and*
- *intentionally exceeded or misused that access in a manner that*
- *negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.*

# Insider Threat Portfolio



MERIT

Fraud, IT Sabotage, IP Theft, and Espionage

Crime Profiles

Onsite Insider Threat Vulnerability Assessment

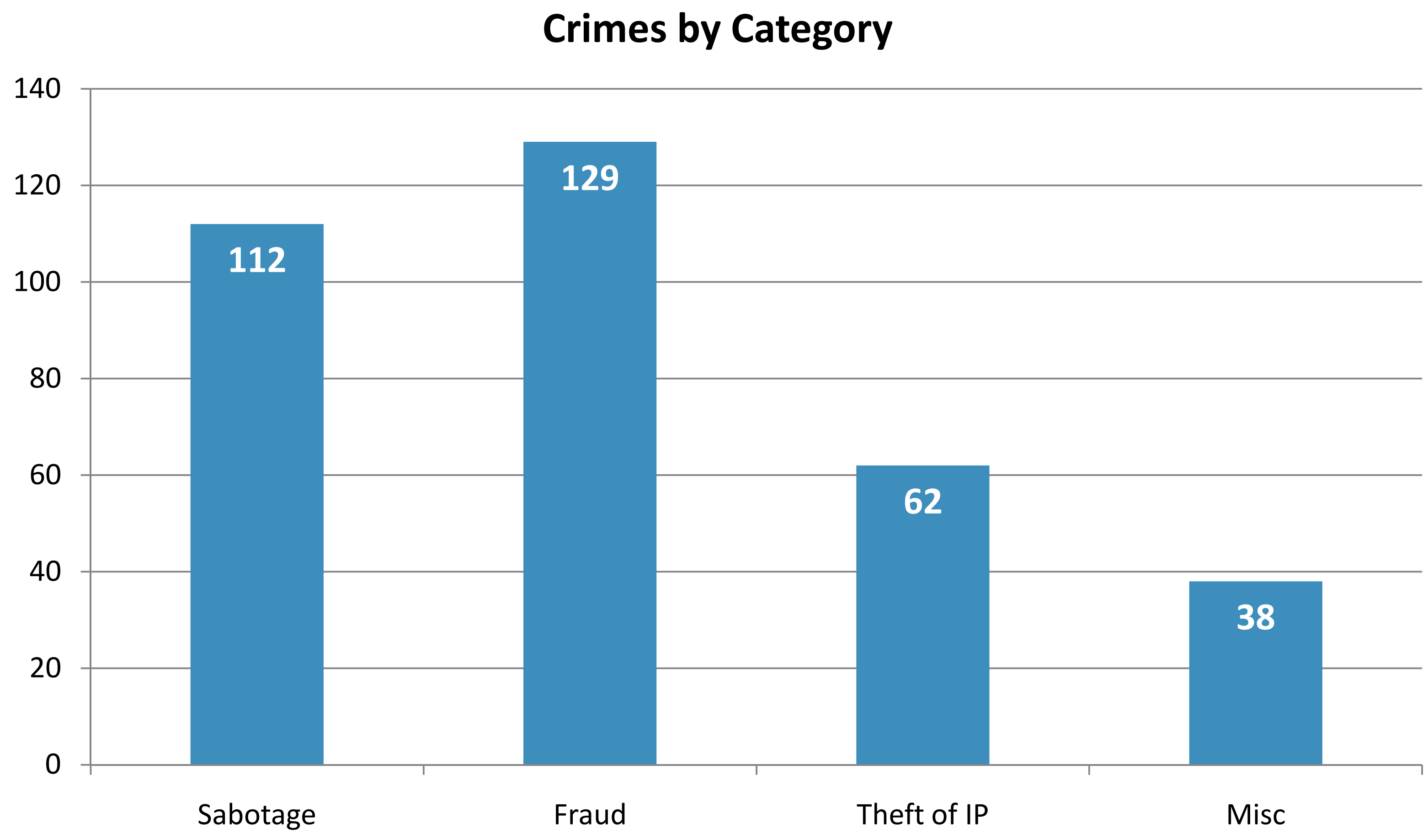
Insider Threat Workshop

Insider Threat Custom Services

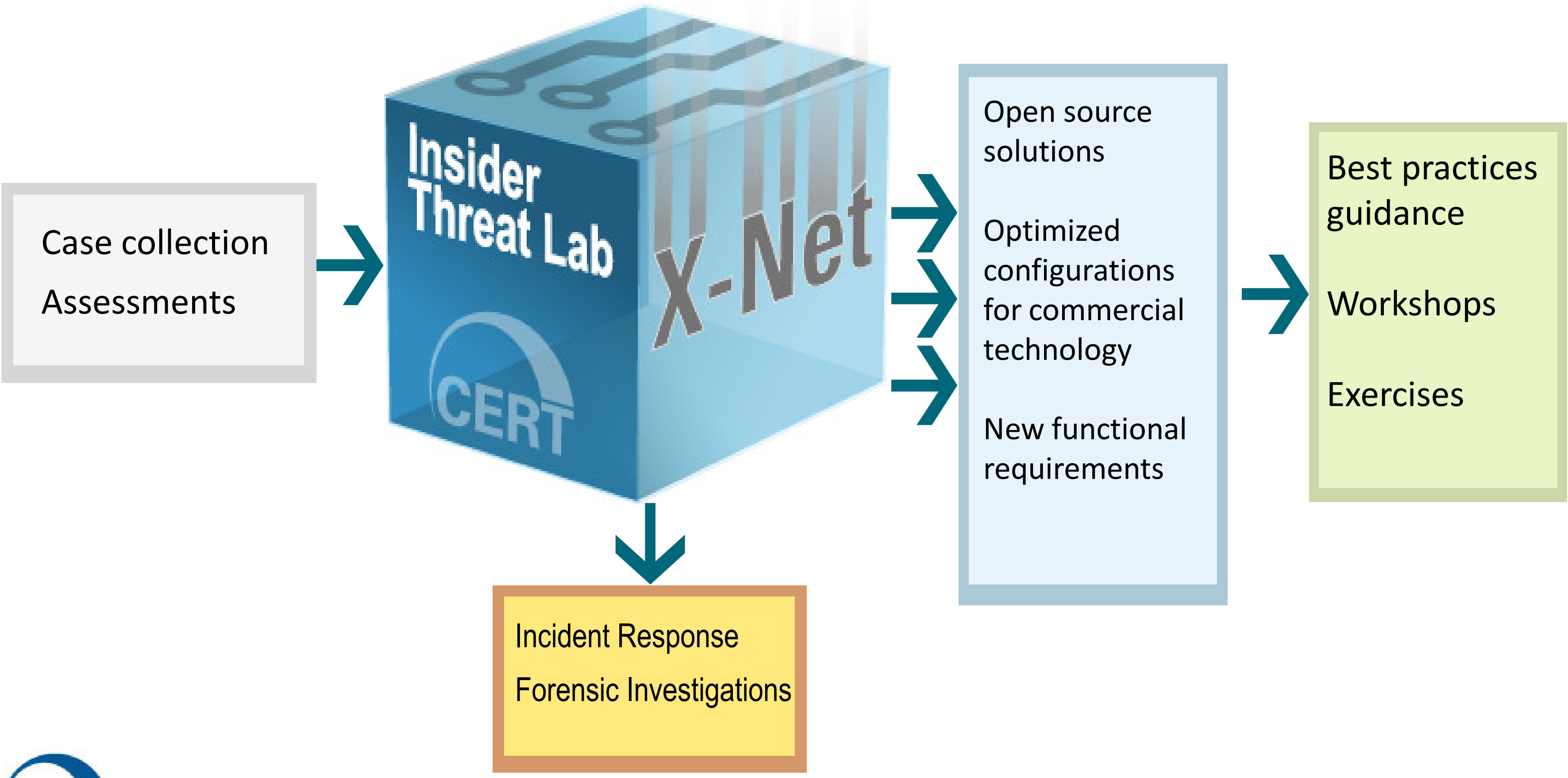
Automated Indications and Warnings

*MERIT – Management and Education of the Risk of Insider Threat*

# MERIT Insider Threat Case Breakdown



# MERIT Insider Threat Lab



Case collection

Assessments

Open source solutions

Optimized configurations for commercial technology

New functional requirements

Best practices guidance

Workshops

Exercises

Incident Response

Forensic Investigations

# Topic of this Session

- More security tools are available, so detection of illicit insider activity should be easier
- BUT: the number of insider incidents continues to grow
- WHY? Insiders have access, knowledge, and opportunity
- Our objective:
  - Present practical strategies for effectively implementing those tools to detect illicit insider activity
  - Present actual case examples and demos

# IT Sabotage

DAN
DAN
SLAM!
Attach File(s)
Do you want to attach DAN_BACKDOOR.EXE?
YES
NO

# Insider IT Sabotage

| | IT Sabotage |
|---|---|
| % of crimes in case database | 34% |
| Current or former employee? | Former |
| Type of position | Technical (e.g. sys admins or DBAs) |
| Gender | Male |

# Insider IT Sabotage - 2

| | IT Sabotage |
|---|---|
| Target | Network, systems, or data |
| Access used | Unauthorized |
| When | Outside normal working hours |
| Where | Remote access |
| Recruited by outsiders | None |
| Collusion | None |

# Unknown Access Paths Used in Actual Cases

- Planted logic bomb while still employed
- Created backdoors before termination or after being notified of termination
- Installed modem for access following termination
- Disabled anti-virus on desktop & tested virus
- Installed remote network administration tool
- Downloaded and installed malicious code and tools (e.g., password cracker or virus)

## Undetected Technical Precursors in Actual Cases

- Downloading and use of “hacker tools” such as rootkits, password sniffers, or password crackers
- Access of web sites prohibited by acceptable use policy
- Use of backdoor accounts
- Set up every new computer so he could access it remotely
- Modification of logs to conceal malicious activity

# Monitoring Strategies for Insider IT sabotage

- Detection of configuration changes
- Alerting of suspicious traffic
- Monitoring for unauthorized accounts

***We've all heard this before…. Then what's the problem???***

# Change and Configuration Control

## *Problem:*

- Privileged users
  - Can insert malicious code just about anywhere and it is not anomalous activity
  - Have the ability to override system controls without detection
- Information overload: can’t realistically monitor everything everyone does online

# Change Control

## *Solution Strategies:*

- Learn from the MERIT models and from past cases
- Implement continuous logging and centralized, secure log server
- Detect and investigate changes that should occur infrequently, e.g.
  - Changes to operating system files, scripts, and executables
  - Changes to stable production systems
  - Services killed on host
- Audit individual actions in logs for privileged accounts
  - Especially for insiders who are “on the HR radar”
- Scan workstations regularly for potentially offensive tools (scanners, crackers, fuzzers, etc.)
- Audit access to backup information and results of backup and recovery tests carefully – this is your last line of defense!

# Actual case examples

***Example#1:*** Malicious code inserted into system utility to steal employee passwords

***Example#2:*** Virus tested on employee's computer before deploying on customer installations

***Example#3:*** Modification of source code disables automated notifications to security department

# Perimeter Controls

## *Problem:*

- Privileged users have solicited assistance from the Internet Underground to commit insider IT sabotage
- Privileged users have used “hacker tools” against their organization
- Security of the physical perimeter is often taken for granted

## *Solution Strategies:*

- Configure Intrusion Detection systems and proxies to alert on suspicious outbound traffic
- Continuous logging
- Audit individual actions in logs for privileged users who are “on the HR radar”
- Audit failed physical access attempts

# Actual case examples

***Example#1:*** Download of “hacker tools” for use in IT sabotage attack

***Example#2:*** Use of IRC chat to exfiltrate credentials

***Example#3:*** Insiders were able to gain unauthorized physical access to areas to steal organization information

# Unauthorized Accounts

## ***Problem:***

- Unauthorized accounts are a common method for gaining access following termination
- Account creation is not anomalous activity for many privileged users
- Account audits are not streamlined and can be very resource intensive

## ***Solution Strategies:***

- Implement scripts to compare all accounts against current employee directory
- Alert on creation of new account and investigate or validate legitimacy of all new accounts on a frequent basis
- Control shared accounts

# Actual case examples

***Example#1:*** Use of backdoor accounts “batman” and “James Bond”

***Example#2:*** Use of VPN accounts belonging to other employees

***Example#3:*** Use of testing, training, and customer accounts

# Demo

# Fraud

Upload files?
YES
NO
GOOD LUCK!
WE'LL MISS YOU!

# Insider Fraud

| | IT Sabotage | Fraud |
|---|---|---|
| % of crimes in case database | 34% | 39% |
| Current or former employee? | Former | Current |
| Type of position | Technical (e.g. sys admins or DBAs) | Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service) |
| Gender | Male | Fairly equally split between male and female |

# Insider Fraud - 2

| | IT Sabotage | Fraud |
|---|---|---|
| **Target** | Network, systems, or data | **PII or Customer Information** |
| **Access used** | Unauthorized | **Authorized** |
| **When** | Outside normal working hours | **During normal working hours** |
| **Where** | Remote access | **At work** |
| **Recruited by outsiders** | None | **½ recruited for theft; less than 1/3 recruited for mod** |
| **Collusion** | None | **Mod: almost ½ colluded with another insider<br>Theft: 2/3 colluded with outsiders** |

# Monitoring Strategies for Insider Fraud

- Detection of unauthorized addition / modification of data in databases

# Unauthorized Data Access / Modification

## Problem:

- Authorized users have added, modified, or deleted data in databases to commit fraud against the organization
- Collusion between employees occurred in approximately 50% of the cases, possibly to overcome separation of duties

## Solution Strategies:

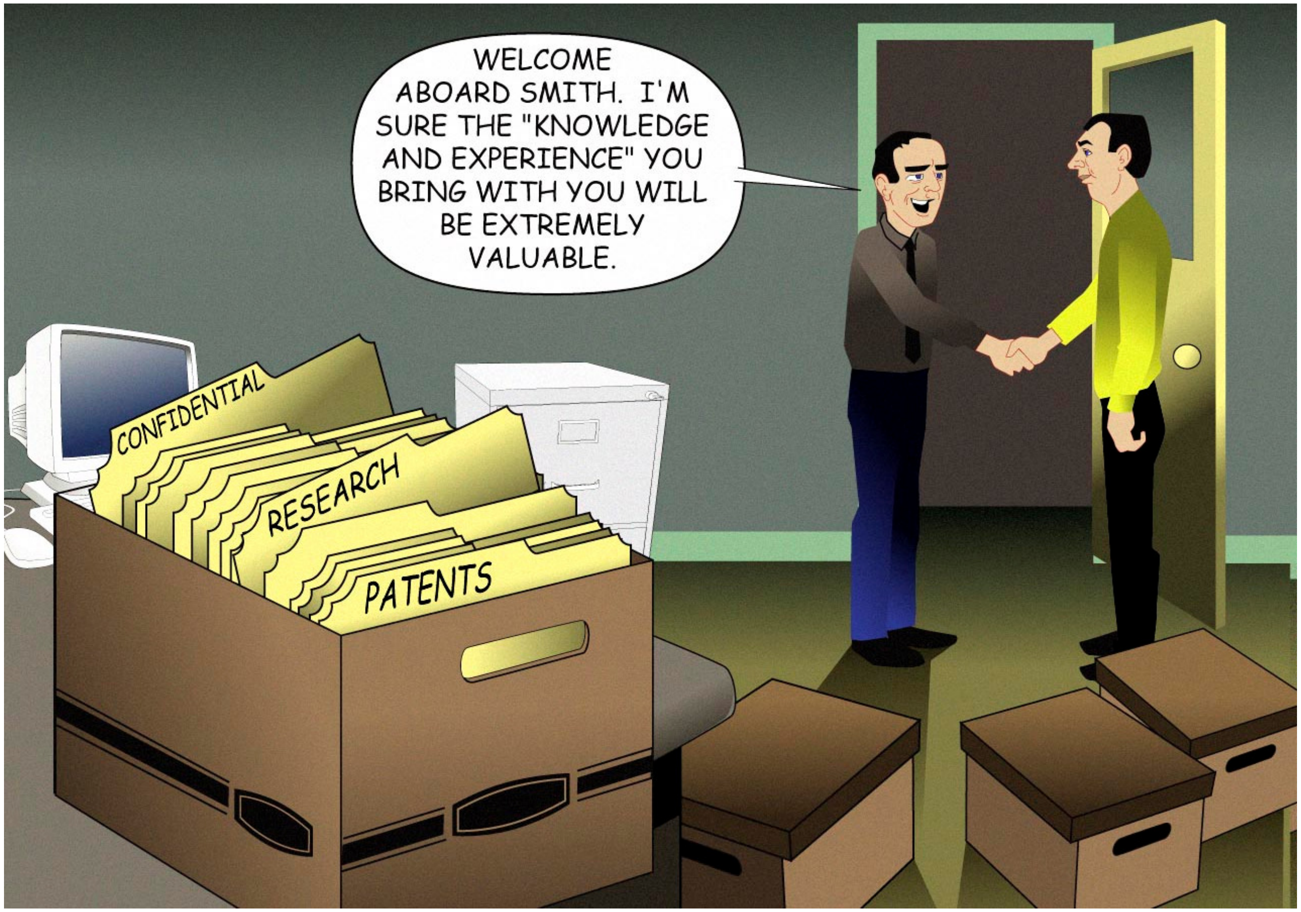
- Auditing database transactions may help detect unauthorized access and modification of data
- Auditing data changes for all tables in a database is not practical and may degrade performance
- Monitor access and data modifications on critical tables, such as tables containing PII or customer information
- Audit either successful or unsuccessful data access / modification attempts or both

# Actual case examples

***Example#1:*** Conspiracy to sell fraudulent driver’s licenses

***Example#2:*** Wiring of money from a dormant bank account into a personal account

# Theft of Intellectual Property


WELCOME ABOARD SMITH. I'M SURE THE "KNOWLEDGE AND EXPERIENCE" YOU BRING WITH YOU WILL BE EXTREMELY VALUABLE.
CONFIDENTIAL
RESEARCH
PATENTS

# Insider Theft of Intellectual Property

| | IT Sabotage | Fraud | Theft of Intellectual Property |
|---|---|---|---|
| **% of crimes in case database** | 37% | 39% | **19%** |
| **Current or former employee?** | Former | Current | **Current** |
| **Type of position** | Technical (e.g. sys admins or DBAs) | Non-tech, low-level positions with access to confidential or sensitive info (e.g. data entry, customer service) | **Technical (71%) - scientists, programmers, engineers**<br>**Sales (29%)** |
| **Gender** | Male | Fairly equally split between male and female | **Male** |

# Insider Theft of Intellectual Property - 2

| | IT Sabotage | Fraud | Theft of Intellectual Property |
|---|---|---|---|
| **Target** | Network, systems, or data | PII or Customer Information | **IP (trade secrets) – 71%**<br>**Customer Info – 33%** |
| **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** |
| **Recruited by outsiders** | None | ½ recruited for theft; less than 1/3 recruited for mod | **Less than 1/4** |
| **Collusion** | None | Mod: almost ½ colluded with another insider<br>Theft: 2/3 colluded with outsiders | **Almost ½ colluded with at least one insider; ½ acted alone** |

# Methods for Exfiltrating Information

- In order of prevalence
  - Copied/downloaded information
  - Emailed information
  - Accessed former employer’s system
  - Compromised account
  - Stole hardcopies
- Many other methods

# More Details on Exfiltration Methods

- Downloaded onto removable media at work, onto laptop from home, using ftp or telnet
- Emailed to competitor, to personal email account, to new employer, using anonymous remailer
- Created backup copy of hard drive
- Gave company laptop to competitor for copying before resignation
- Stored information on password-protected website at work
- Software and hardware keystroke loggers

# Monitoring Strategies for Insider Theft of Information

- Detection of data leakage
- Detection of unauthorized devices
- Monitoring for remote access attempts

***We've all heard this before….***

***There are lots of Data Leakage Prevention tools …***

***Then what's the problem???***

## Data Leakage

### *Problem:*

- Massive volume of data makes monitoring and alerting difficult
- Difficult to baseline normal behavior and configure tools to identify abnormal behavior
- Insiders tend to steal the same data they access in the course of the normal workday

# Data Leakage -2

## Solution Strategies:

- Learn from the MERIT models and from past cases
- Log, monitor, and audit system logs for queries, downloads, print jobs, email messages containing unusually large amounts of data, PII, and proprietary information
- Alert on emails to competitors, foreign locations, or personal email accounts
- Monitor network flow data for abnormally large file transfers, long connections, odd ports, illegal source/destination IP addresses, …
    - Then review pcap data to reconstruct content of transactions.
    - First need to measure the network baseline so “normal” baseline is defined, including who should be talking to whom

***Implement targeted monitoring of individuals who are “on the HR radar” or “on the way out the door”***

# Actual case examples

***Example#1:*** Use of FTP to exfiltrate customer credit card information

***Example#2:*** Use of email to exfiltrate trade secrets

***Example#3:*** Downloading proprietary information from a database

# Rogue Devices or Removable Media

## *Problem:*

- Organizations may not detect unauthorized devices connected to their networks
  - Peripherals, e.g. keyloggers, removable media, backup systems, modems
  - Network devices, e.g. rogue laptops, access points, mobile devices
- It can be difficult to distinguish between legitimate and illegitimate use of removable media
- Laptops are a common means of intentional data exfiltration

# Rogue Devices or Removable Media

## *Solution Strategies:*

- Audit logs for activity of resigning or terminating employees
  - Learn from the MERIT models and from past cases
  - Log all downloads to removable media
  - Alert when critical information is downloaded to removable media, e.g. intellectual property, customer information, PII
  - Log anytime a device or peripheral is attached; alert if unidentified device is attached, such as keystroke logger
  - Use monitoring tools on laptops that "phone home" when connected to the network
  - Consider prohibiting the use of personal devices for work-related activities

# Actual case examples

***Example#1:*** Proprietary source code copied to removable media

***Example#2:*** Terminating employee allows new employer to make copy of entire laptop just prior to resignation

***Example#3:*** Hardware keylogger used to steal confidential information from CEO

# Remote Access Attempts

## *Problem:*

- Privileged employees are able to create unknown access paths for access after termination
- Disabling all access paths for a terminating employee is a difficult task if constant account management practices are not followed.

## *Solution Strategies:*

- Learn from the MERIT model and from past cases
- Implement targeting monitoring of prior online activity of individuals who are “on the way out”
- Log, monitor, and audit for remote access from IP addresses from outside the U.S., from competitors’ networks, and from terminating or terminated employees

# Actual case examples

***Example#1:*** An employee was able to access a former employer's system because of a failure to detect / disable remote access software he had installed while employed.

***Example#2:*** A former employee was able to connect to the organization's network and exfiltrate information from a competitor's network (outside the U.S.)

# Application to your Organization

- Many organizations are able to log the majority of online activity

but

- Many organizations do not have the resources, including software, hardware, and people, to consistently audit and monitor all online transactions

# Application to your Organization

- The challenge to organizations is to use a combination of technical and non-technical potential indicators of malicious activity to identify individuals who may be more at risk of committing an insider crime

and then

- Apply the auditing and monitoring strategies outlined in this presentation

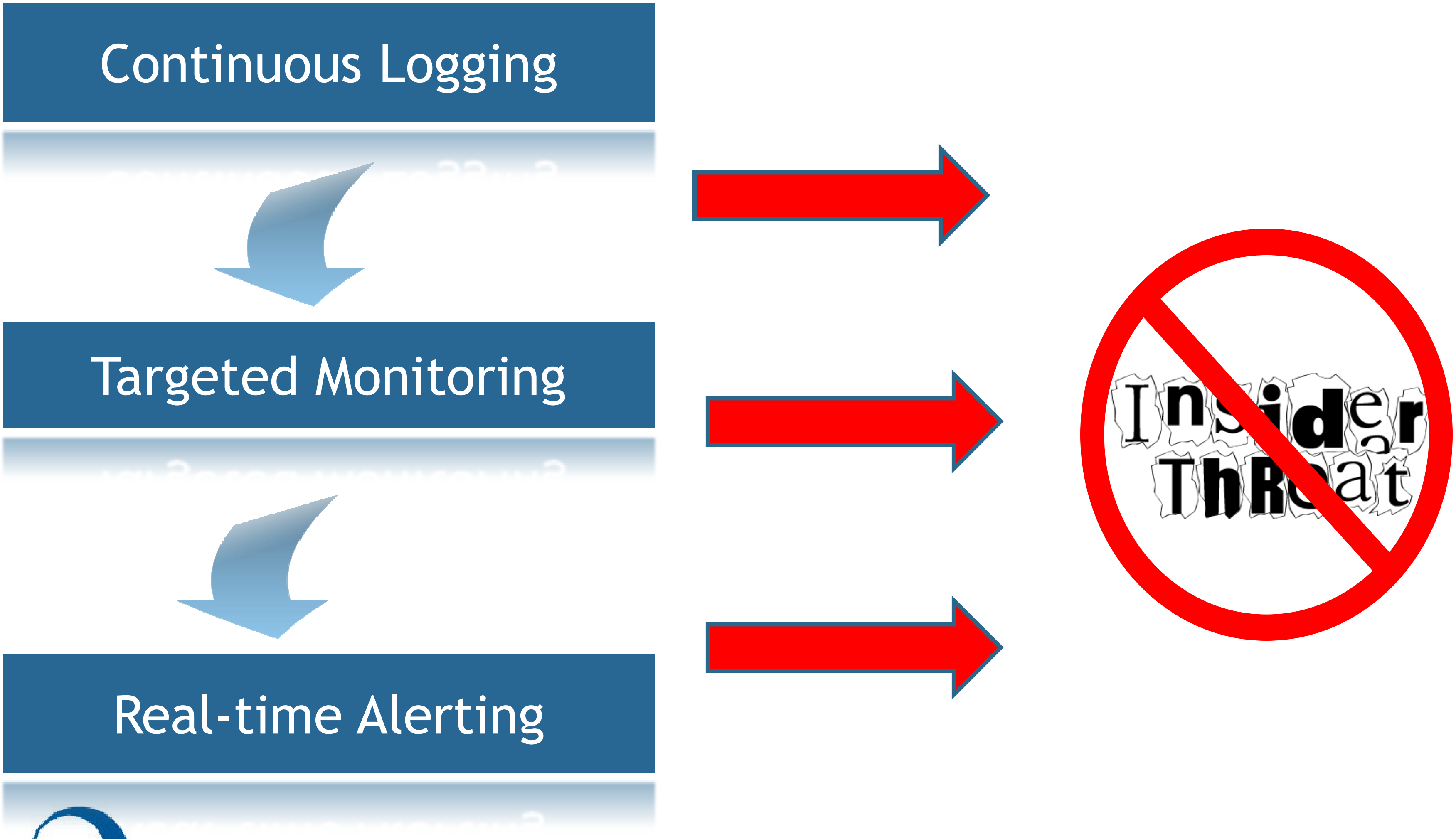
# Application to your Organization

- The good news is that most of the monitoring solutions suggested in this presentation can be implemented using existing tools, technologies, and staff
- But it does require new processes for communication between HR, IT, Information Security, Legal, Physical Security, management, … regarding employee issues
  - Employees on the HR radar
  - Employees who are about to be terminated, have resigned, have been laid off, …

# Final Thoughts

- Caveats:
  - We only have data on criminals
    - Our findings / recommendations could result in a high false positive rate
    - We would like to work with organizations that are willing to be pilot sites – please contact us!!
  - These monitoring techniques are not a guarantee
    - In the event of a missed insider attack, these methods will be tremendously beneficial for incident response and forensic analysis teams
  - Consider legal, privacy, and policy issues before implementing any employee monitoring  program
- Food for thought:
  - Which of the monitoring techniques we've presented might also be effective in detecting external intruders if they manage to gain access?
  - Could these controls be effective against both insiders and outsiders?

# Our Suggestion



Continuous Logging

Targeted Monitoring

Real-time Alerting

# Points of Contact

**Technical Manager, Threat and Incident Management**
Dawn M. Cappelli, CISSP
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-9136 – Phone
dmc@cert.org – Email

**Team Lead, CERT Insider Threat Team**
Randy Trzeciak
Senior Member of the Technical Staff
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/

Insider Threat