The 46th Annual IEEE International Carnahan Conference on Security Technology

Standing up an Insider Threat Program

Jointly presented by MITRE and CERT

Notices

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT ® is a registered mark owned by Carnegie Mellon University.

Outline of the Tutorial

- Introductions
- Definition of Insider Threat
- What does an Insider do?
- Motivation/Goals for a Program
- Definition of a Program
- Data Sources
- Insider Threat Analysis
- Preventative and Detection Mechanisms
- Assessing a Program Discussion

Introduction

What is an FFRDC?

Federally Funded Research and Development Center

- Operates as strategic partners with their sponsoring government agencies
- Organized as independent entities with limitations and restrictions on their activities
- Assists U.S. government with scientific research and analysis, development and acquisition, and systems engineering/integration
- Brings together the expertise and outlook of government, industry, and academia to solve complex technical problems

What is MITRE?

A not-for-profit corporation, chartered in the public interest, that is a collection of individual FFRDCs sponsored by:

- the National Security Engineering Center for the Department of Defense;
- the Center for Advanced Aviation System Development for the Federal Aviation Administration;
- the Center for Enterprise Modernization for the Internal Revenue Service and U.S. Department of Veterans Affairs;
- the Homeland Security Systems Engineering and Development Institute for the Department of Homeland Security; and
- the Judiciary Engineering and Modernization Center for the U.S. Courts

Cyber Security Division Insider Threat Capability

- Provide methods for identifying, assessing, and mitigating the insider threat
- Work to integrate best practices across a diverse sponsor base

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

Part of the Software Engineering Institute (SEI)

- Federally Funded Research & Development Center (FFRDC)
- Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

What is the CERT Insider Threat Center?

Center of insider threat expertise

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

Our mission: *The CERT Insider Threat Center conducts empirical research and analysis to develop & transition socio-technical solutions to combat insider cyber threats.*

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.*

Note: This workshop does not address national security espionage involving classified information

Insider Threat Issue -1

Insiders pose a substantial threat by virtue of their knowledge of, and access to, their employers' systems and/or databases.

Insiders can bypass existing physical and electronic security measures through ***legitimate*** measures.

Insider Threat Issue -2

How many of your organizations have been victim of an insider attack?

How many of your organizations can ***confidently*** say you have ***not*** been the victim of an insider attack?

Insider Threat Issue -3

Many organizations feel they have to choose between protection from outsiders versus insiders.

Keep in mind that once an outsider gets in, there is a good chance they will perform the same types of malicious acts as malicious insiders, for example:

- Plant malicious code or logic bomb
- Create backdoor account
- Exfiltrate intellectual property or other proprietary information

Therefore, insider threat controls can also provide protection from outsiders.

The Expanding Complexity of “Insiders”

Area	Description
Collusion with outsiders	Insiders recruited by or working for outsiders, including organized crime and foreign organizations or governments
Business partners	Difficulty in controlling/monitoring access to your information and systems by “trusted” business partners
Mergers & acquisitions	Heightened risk of insider threat in organizations being merged into acquiring organization
Cultural differences	Difficulty in recognizing behavioral indicators exhibited by insiders working for US organizations who are not US citizens
Foreign allegiances	US organizations operating branches outside the US with the majority of employees who are not US citizens

Many Motivations

Authorized users, authorized actions

Authorized users, *unauthorized* actions

***Unauthorized* users, authorized actions**

***Unauthorized* users, *unauthorized* actions**

- **Carelessness**
- **Curiosity**
- **Promote Change**
- **Personal Gain / Motive**
- **Idealism**
- **Political rationale**
- **Revenge / Sabotage**
- **Control / Power**
- **Profit**
- **Blackmail**
- **Foreign or state-sponsored goals**

Types of Insider Crimes -1

Insider IT sabotage

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

Insider theft of intellectual property (IP)

An insider's use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders.

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 (identity theft, credit card fraud).

Types of Insider Crimes -2

Insider IT sabotage

- Deletion of information
- Bringing down systems
- Web site defacement to embarrass organization

Insider theft of intellectual property

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

Insider fraud

- Theft and sale of confidential information (SSN, credit card numbers, etc.)
- Modification of critical data for pay (driver's license records, criminal records, welfare status, etc.)
- Stealing of money (financial institutions, government organizations, etc.)

Types of Insider Crimes -3

Miscellaneous

- Disclosure of information insider believed should be in the public domain
- Query of database to find address of person – information provided to acquaintance who physically harmed individual
- Query of high-profile individuals to access personal information

National Security Espionage

- Spies against the U.S.

An Example of IT Sabotage

911 services disrupted for 4 major cities

Disgruntled former employee arrested and convicted for this deliberate act of sabotage.

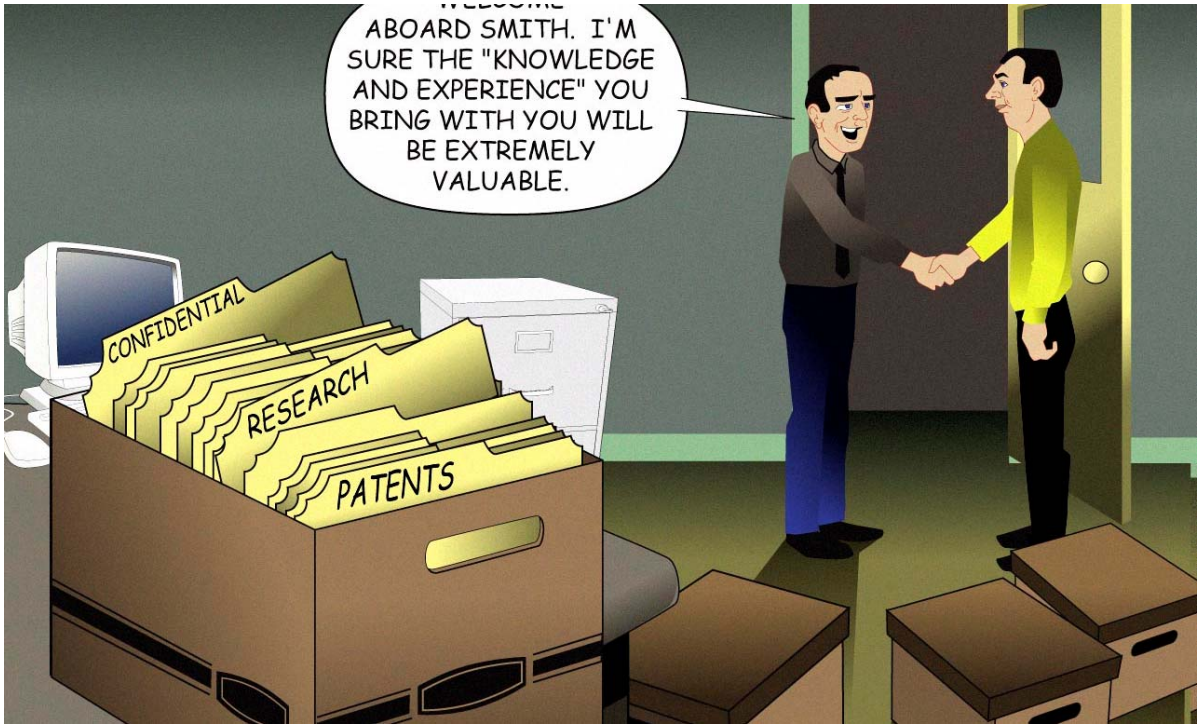
An Example of Insider Fraud

Fake drivers license sold to undercover agent claiming to be on the "No Fly list"

An Example of Theft of Intellectual Property

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



Policy and Authority

Authorities

- Title 18 - Crime
  - 18 USC 793 US Code – Gathering, transmitting or losing defense information
  - 18 USC 794 US Code – Gathering or delivering defense information to aid foreign government
  - 18 USC 798 US Code – Disclosure of Classified information
- Section 811 1995 Intelligence Authorization Act
  - Immediate notification to the FBI whenever there are indications that classified information may have been disclosed without authorization to a foreign power. (non-DOD)
- UCMJ 106a Espionage (Title 10 US Code 906a)
- Section 922 2012 National Defense Authorization Act
  - DOD required to establish a program for information sharing protection and Insider Threat mitigation for DOD systems.
- Executive Order #13587

MITRE

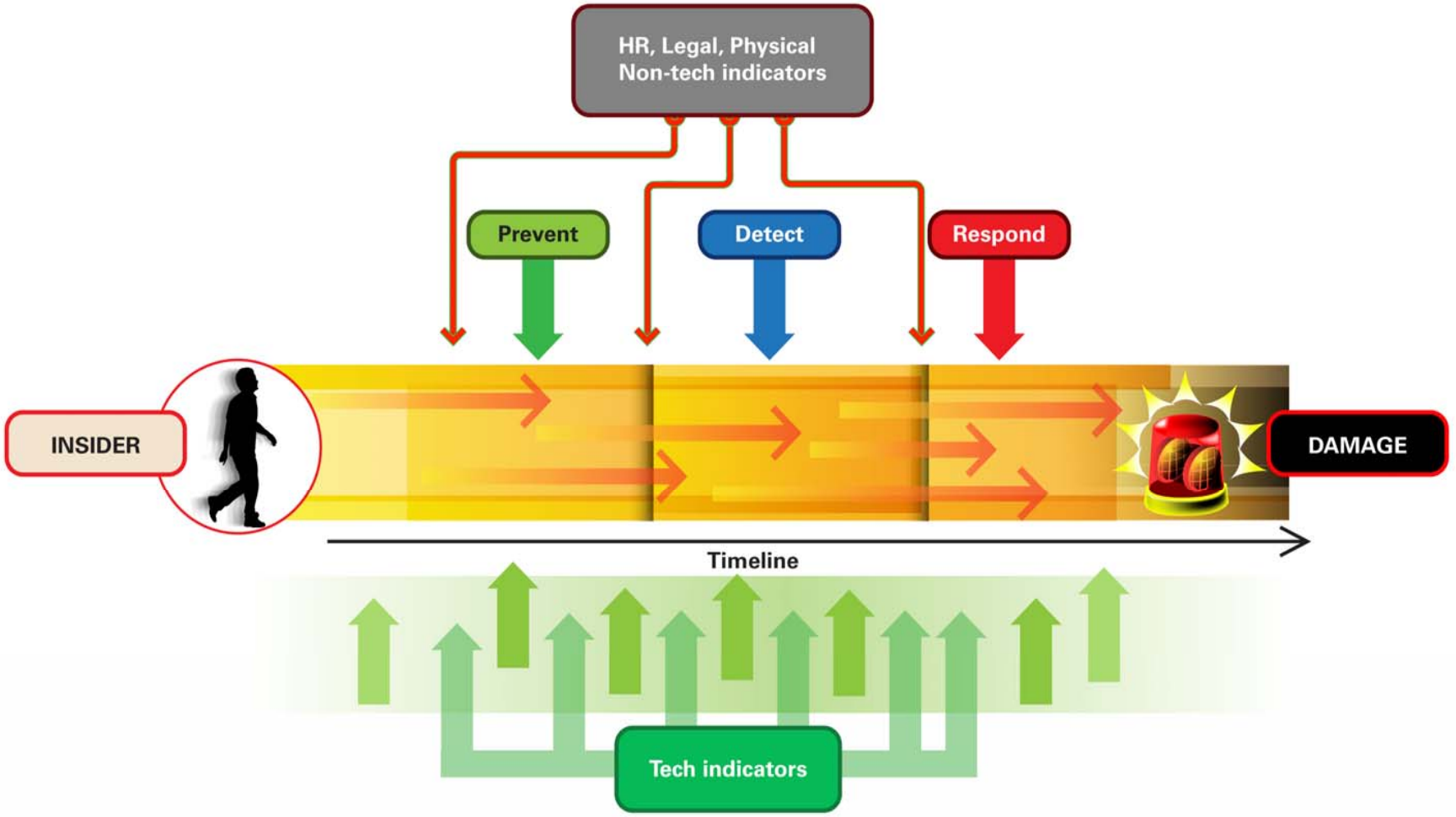
Policy and Authority

Policies

- **Organization Log/Auditing Policy**
  - **Provides policies for responsibility of organization's offices and programs to supply auditing information to central log gathering and aggregating component.**
  - **Provides for responsibility to collect and store audit data and for how long**
- **User acceptable use policies**
  - **Privileged User Rules of Behavior**
  - **Regular User Rules of Behavior**
- **Privacy Impact Assessments (PIAs)**
  - **Typically, auditing systems of record and dealing with sensitive personnel issues would necessitate the need to handle personally identifiable information (PII)**

Components of an Insider Threat Program

Goal for a Program



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

Motivation for a Program

"to ensure the responsible sharing and safeguarding of classified national security information on computer networks." Source: Executive Order 13587, quoted in GCN (http://s.tt/1ai6l)

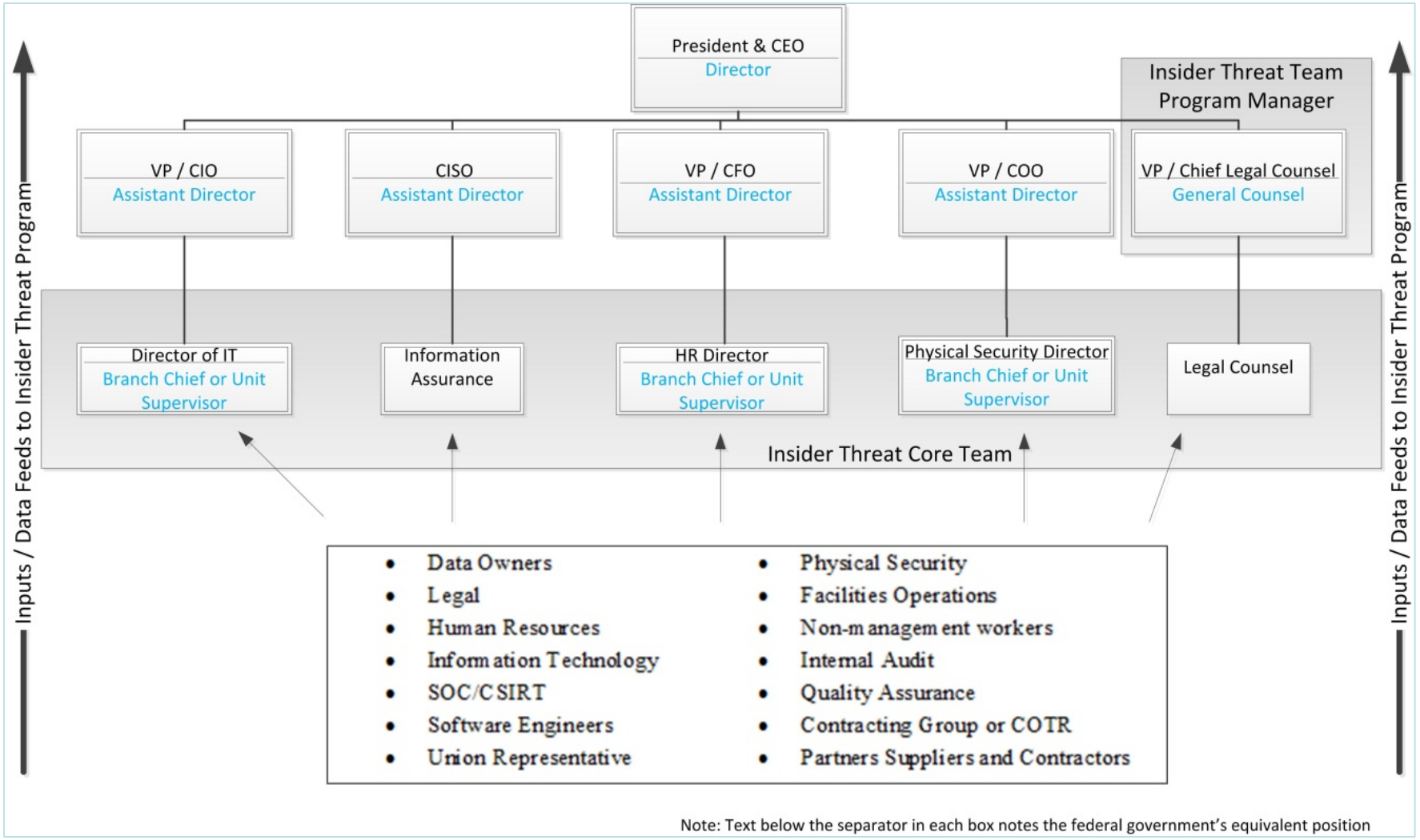
To ensure protection of and appropriate access to intellectual property and other critical assets, systems, and data including

- people
- business processes
- technology
- facilities
- information

To be prepared and ready to handle such events in a consistent, timely, and quality manner including understanding

- who to involve
- who has authority
- who to coordinate with
- who to report to
- what actions to take
- what improvements to make

Insider Threat Program Participants (Notional)



Insider Threat Components – Legal

General Counsel

- Policies
- Procedures
- Incidents
- Training/Awareness/Reporting
- Privacy & Civil Liberties

Insider Threat Components – HR

Biographic Information

- Personal identifying data
- Employment identifying data
- Job Title
- Supervisor
- Start/End Dates

Expanded Data (case-by-case)

- Performance
- Compensation

Insider Threat Components – Security

Physical Security

- Facility Access
- Incident Data

Personnel Security

- Adjudication
- Privileged Access
- Foreign Contacts
- Foreign Travel
- Finances
- Polygraph
- Behavioral Sciences

Insider Threat Components – IT/IA

User Monitoring of IT Systems

- Logon/Logoff
- Data Access
- Data Movement/Manipulation
  - Printing
  - Removable Media
  - Email Attachment
  - Encryption
  - Steganography
  - Denial
  - Deception
- Account Manipulation
- Bypassing Security

Insider Threat Components – Training

Insider Threat Training

- Policy Reinforcement
- Awareness
- Reporting
  - Procedures
  - Results
- Logging

Insider Threat Components – Response

Analysis

- Collection and synthesis of disparate data sources
- Fusion and analysis

Reporting

- For Record
- Referral
- Disposition

Response

- Mitigation
- Remuneration

Insider Threat Program Development

Key aspects of our model program:

1. Policy, Authority
2. Prevention, Collection
3. Personnel Review, Threat Awareness, Analysis, Attribution
4. Incident Response, Investigation

- CND
- Security
- LE/CI

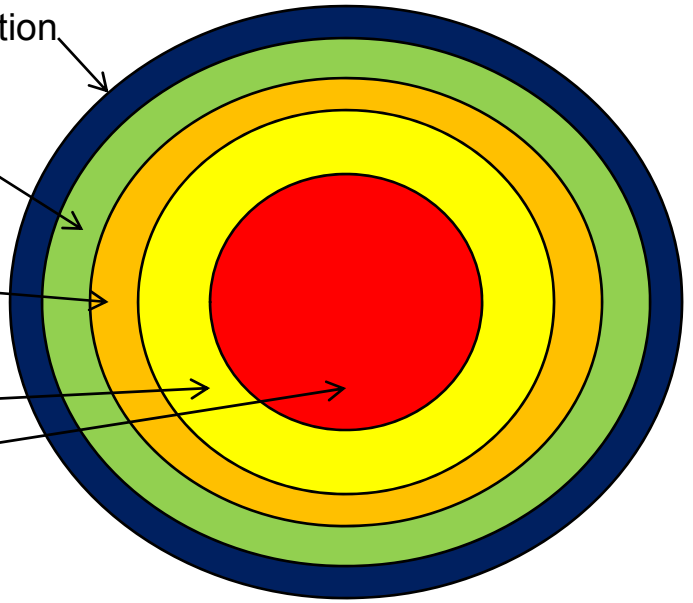
MITRE

Insider Threat coupled with Audit

- **Traditionally, Insider Threat has been an issue tackled using advanced auditing methods.**

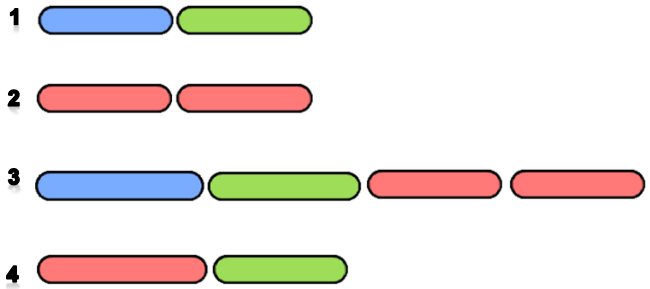
- **There is an assumption that there exists a mature auditing program**

  - Perimeter Monitoring: Firewalls, Intrusion Detection
  - Operating System auditing: Syslog, EventLog, Host-based monitoring
  - Application auditing
  - Special System auditing: network Logon/Logoff PKI, Badging
  - High Value Targets (HVTs)



Program Aspects

- Depending on many factors such as type of program or responsible entities, programs may not have all aspects.
- Most successful programs will have most aspects at well-developed maturity level.
- Although a particular aspect is not always present, implementers should as least identify, consider and/or remediate missing aspects.



MITRE

Typical Roles (1/2)

CND Administrator
Deploys and operates CND auditing and preventative data sources.
Responsibilities are to deploy and maintain the sensor grid. Would likely be used during incident mitigation. Has permissions to make changes to enclaves that they are responsible for.

Insider Threat Analyst
Performs technical analysis of the data to assess for necessary escalation.
Typically these are tiered subject matter experts at interpreting information from auditing sources and human behavior that is indicative of a problem.

MITRE

Typical Roles (2/2)

Insider Threat Engineer
Architects and engineers advanced capabilities for pursuing the malicious insider.
Engineer with subject matter expertise in Insider Threat mitigation, auditing, correlation, large datasets and databases, and building complex automation systems.

Law Enforcement/Counterintelligence Agent
Agent of the government that is chartered and empowered to enforce the law.
Typically leads Counterintelligence and espionage investigations. Not technical role.

Data Sources

MITRE

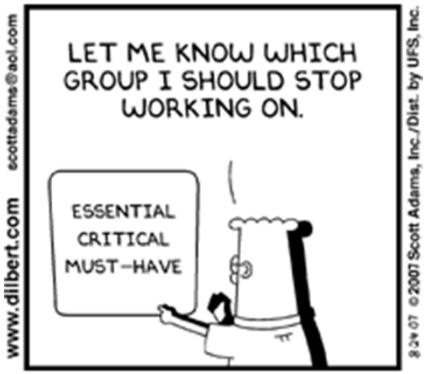
What data do you want?

- Data that helps you do better auditing.
- Some audit data provides no value to an audit group.
- Key is to focus on data that fills any known gaps.

MITRE

Data Prioritization

- Importance
  - Crown Jewel Assessment or Decree
- Difficulty
  - Technical
  - Political
- Resources
  - Personnel
  - Equipment
- Reassess every quarter



MITRE

Solid identification and attribution

- Our model program needs all collected events to be attributed to an identity.

- This requires sustained collection of identity information to cross-reference collected events of interest against.
  - Log data from disparate systems may use different identity information
  - Start Time and End Time for all attributes

- As more identity information is collected, the system becomes more resistant to impersonation.

Identifier
- names
- usernames
- email addresses
- phone numbers
- addresses
- PII

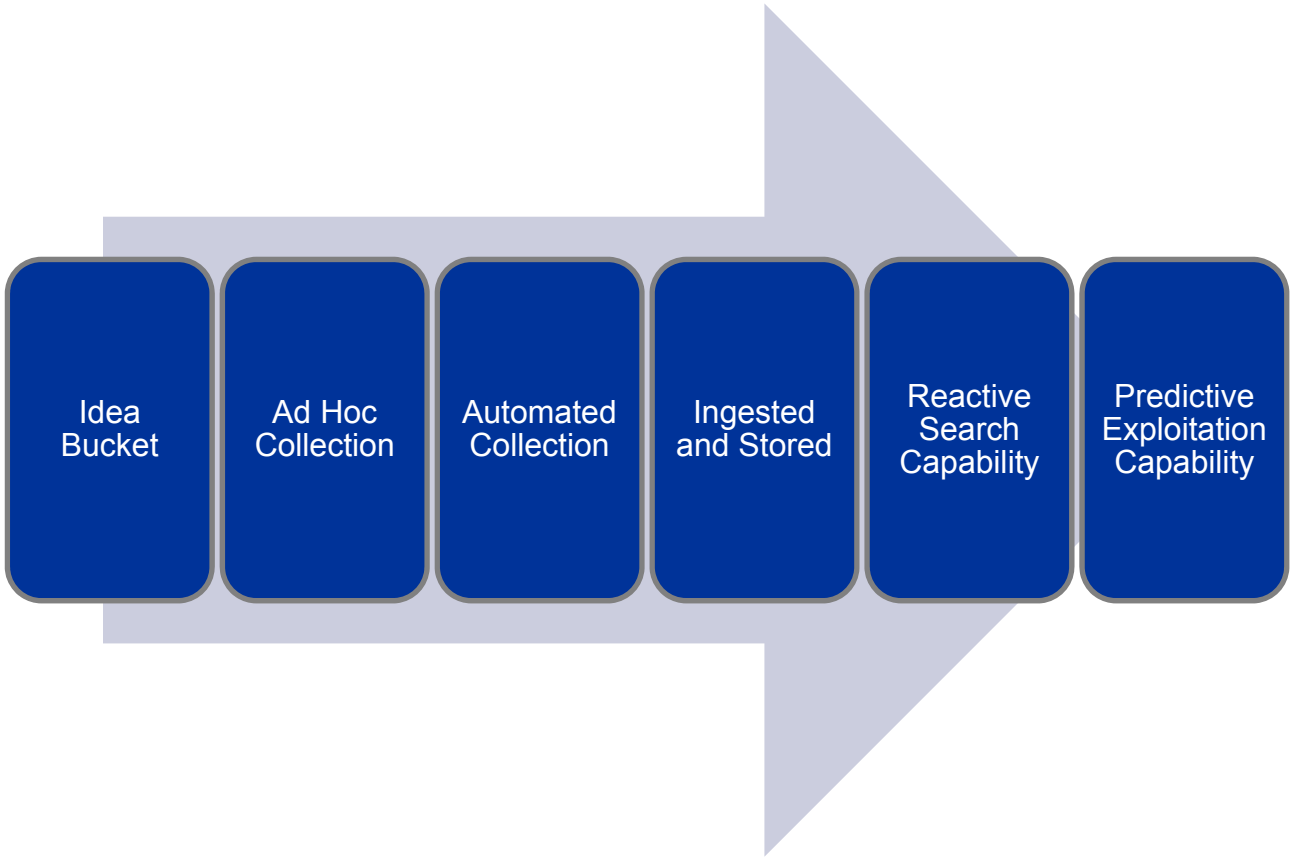
Centralizing Disparate Data

- **Successful programs have merged many disparate data sources**
- **Our model program would deploy Security Information and Event Management (SIEM) technology across many different types of audit sources**
- **The goal would be to normalize data for:**
  - **time synchronization**
  - **attribution**
  - **correlation**

High Value Target Analysis

- What data is critical to your mission?
- What data is critical/important to your adversary?
- Who has access to critical data?

Data Source Maturity Levels



MITRE

Data Formats

- Database
- Flat File
- Proprietary
- Main Frame
- Syslog
- Binary
- Paper Documents
- XML

MITRE

Some Data Issues

- Audit rarely “owns” the data.
- Data tends to be awful.
- And you get a lot of it.
- Finding what you want is a constant challenge.
- Storage and retention become issues as well.

Data Ownership

- Who is in charge of all this data?
  - Most of the time it is not the people responsible for auditing the enterprise.
- How do you get everyone to play nicely?
  - You do not want to take over their fiefdom. You just want to support them and help them go through all their log data.

How do you get this data?

- Sneaker Net is a valid solution.
  - Extremely time consuming.
- Automated Push or Pull.
- An OWT solution depends on the data.
  - Type of data
    - Full packet capture is much different then Small log files.
  - Amount of data
    - Packet Capture could easily be 20GB an hour.
  - Throughput of OWT
    - If you are collection on a 10GB link what's going to happen if your OWT can only handle 100MB.

To ETL or Not?

- Store the raw format, but then what.
- Should you transform to a standard format?
- Or build custom handles for the raw formats?
- Something in between?

What do with the data once you have it?

- **Why … Store it, of course!**

MITRE

Data Retention Policy

- How long do you store the data for?

Long-term Storage

- **Many incidents and investigations rely on data that could be years old.**

- **Our model program would have both the policy and technical mean for long-term storage of audit data. For example:**
  - **25 years**
  - **Length of service of longest employee**

Effective On Duty:
September 1985
Spy Activity
1985 - 2001

Effective On Duty:
January 1976
Spy Activity
1979 - 2001

Common Sources (1/2)

Source	Type	Comment
Perimeter Firewall, IDS logs, web/proxy logs	Audit	Limited use for InT
Syslog, Eventlogs	Audit	Log events do not map well to user actions
Host Based Monitoring	Audit	Augments system logs with more user oriented events
Data Loss Prevention	Audit/Prevention	Can block/prompt/encrypt/log any user oriented event
Application logs	Audit	Provide audit of important network functions or data.
Badge logs	Audit	In/out, attempts, denies, rooms, corridors, stairwells, elevators, etc.

Common Sources (2/2)

Source	Type	Comment
Personnel information	Security	Citations, polygraph inconclusive/failures, financials/debts, promotions/demotions, letters of censure, security or other reportable incidents
Travel	Security	Foreign, international hubs, discrepancies between reported and actual
Privileged User Monitoring	Audit	Difficult to perform on standard data types. Typically, this involves a new product such as a DLP product to collect this information.

Integration Guidance

- When possible, a program should generate integration guidance for the enterprise.
- All organizations are different, but having integration guidance for any new potential audit source enables the program to grow as needed.
- Integration guidance will also help delineate what any new programs will be expected to provide.

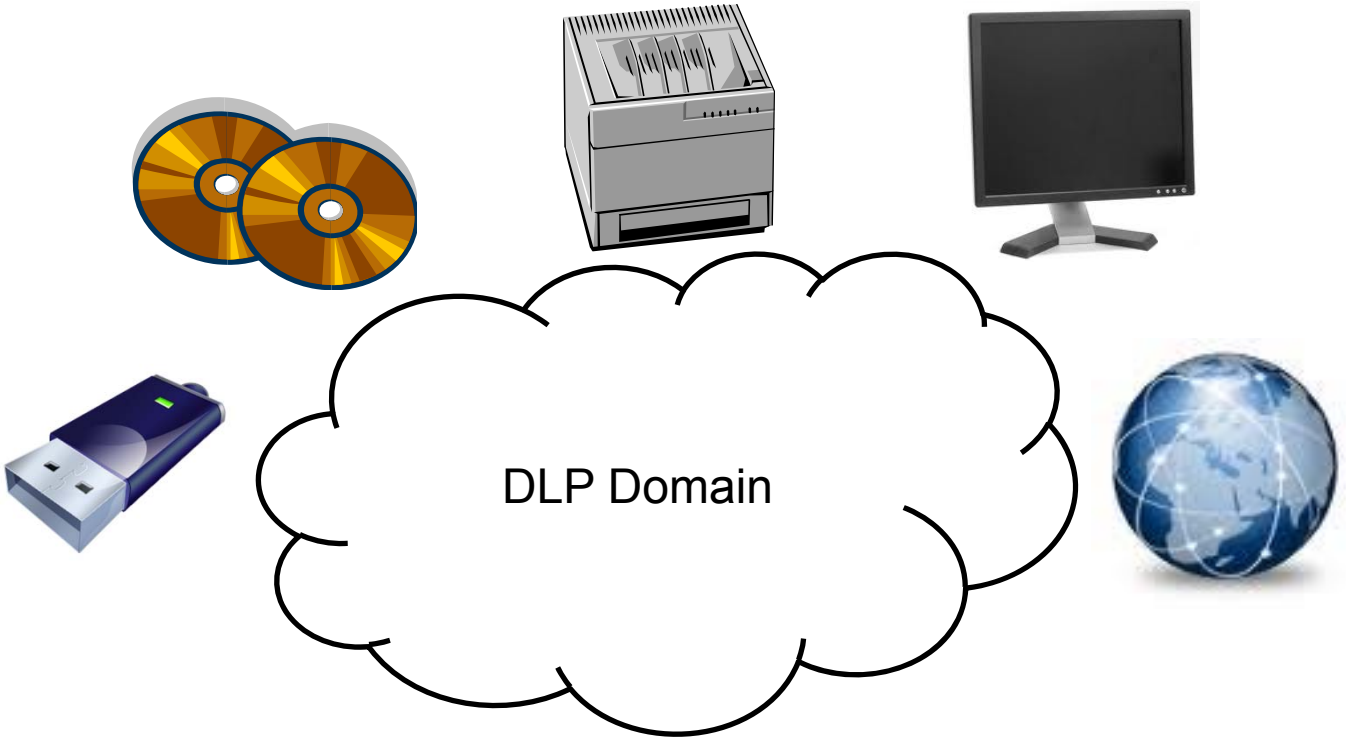
Preventative and Detection Mechanisms

MITRE

Active Prevention to Complement Monitoring

- **Many sponsors have found Data Loss Prevention (DLP) technologies harmonizing with goals of InT auditing**
- **Our model program would deploy a DLP solution on all hosts on every enclave in our boundary**

Advanced Data Loss Prevention



As data moves in and out of the domain, the most advanced solutions can deny, log, prompt for a reason, and even seamlessly encrypt the data so that it cannot be viewed outside of the DLP domain.

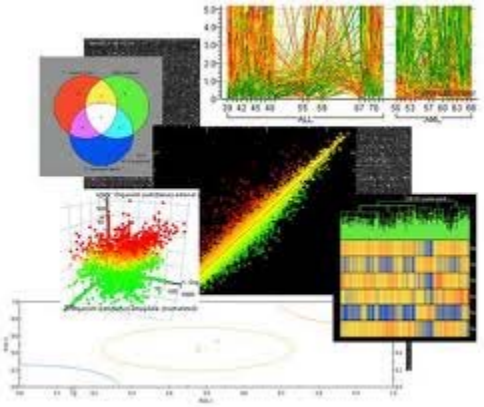
MITRE

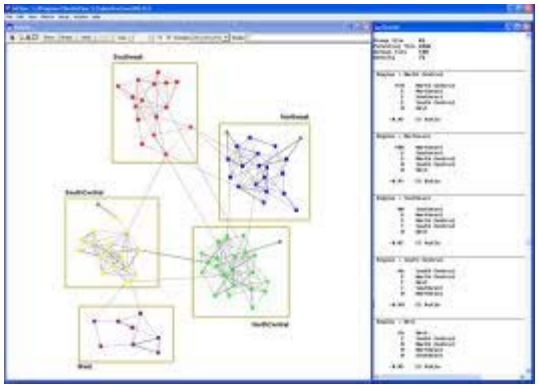
Analysis

MITRE

After you store data, what then?

- You analyze it.
- But what are you looking for?
- And what are your options for action?





MITRE

Cyber Observables

Focus on traits that can be observed and recorded:

ANA MONTES
DIA Analyst convicted 2002 of committing espionage (Cuba).
Encrypted communication

ROBERT HANSSEN
FBI Agent convicted 2001 of committing espionage (Russia).
Numerous self searches, password cracking, OPR

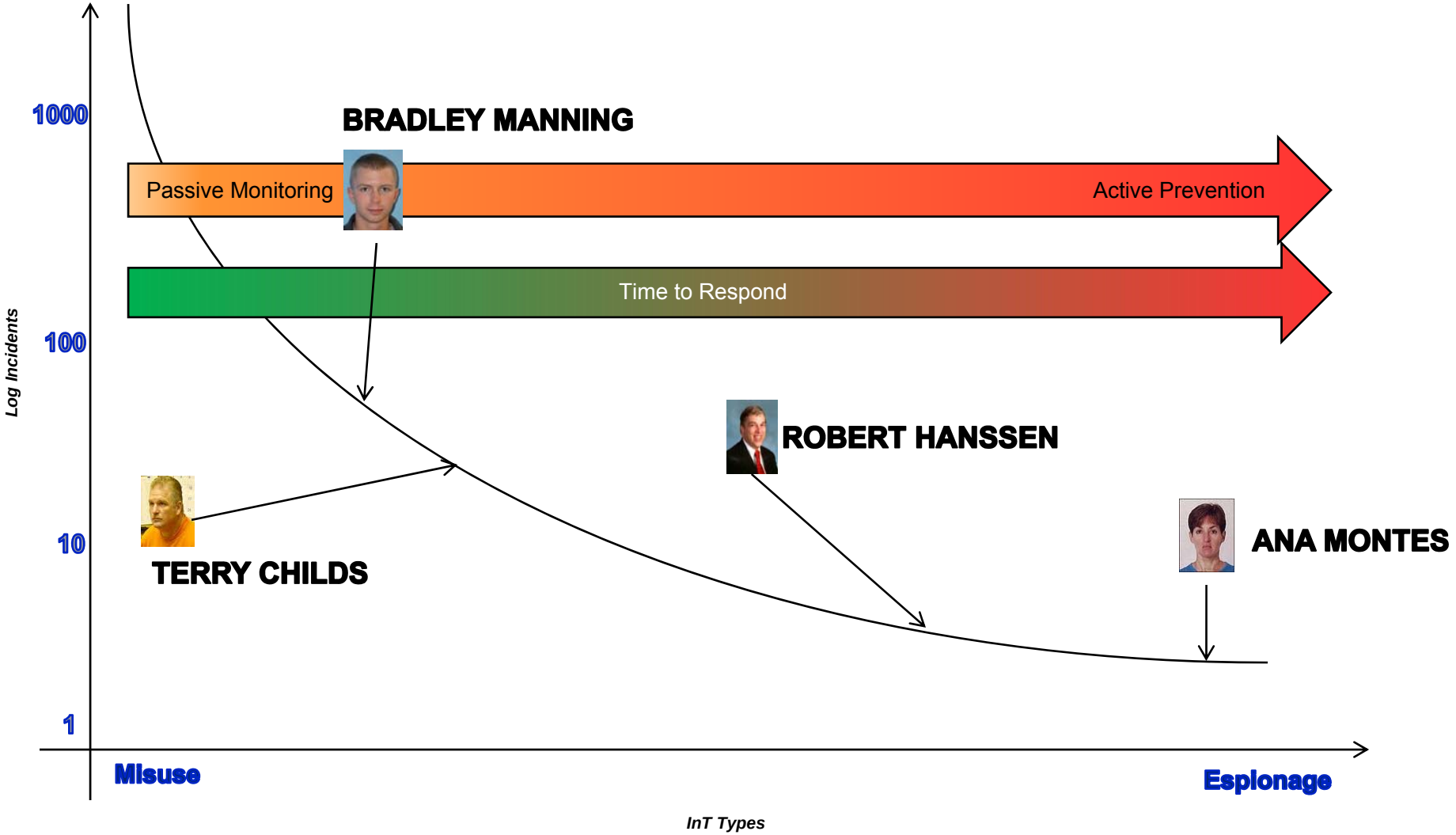
TERRY CHILDS
Network Administrator convicted 2010 for Network Tampering.
Network tampering, subversively avoiding audit checks

BRADLEY MANNING
Army Intel Analyst arrested 2010 for disclosure of classified Information.
Downloaded significant amounts of data, removable media usage

The best programs study past Insider Threat/espionage investigations for application of new indicators.

MITRE

Insider Threat Types



MITRE

Analysis

- **Historically, malicious insiders were identified by either Counterintelligence source reporting or a concerned observer. These then turn into investigations after the fact.**
- **Typical programs have developed bounded processes for tiered triage.**
- **Our model program would employ both reactive and proactive investigative techniques and a clear process for triage.**

Real Time vs Forensic Need

Real Time

Visualization

Alerts

Trending

Dashboard

Search

Historical data

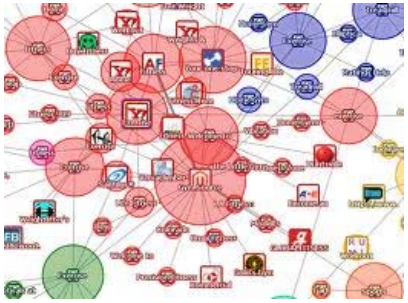
Historical Incident

Data Correlation

MITRE

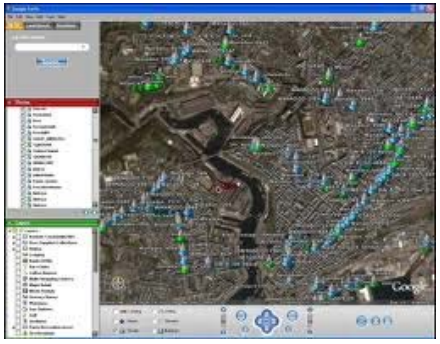
Forensic / Post-Event

Visualization



Link

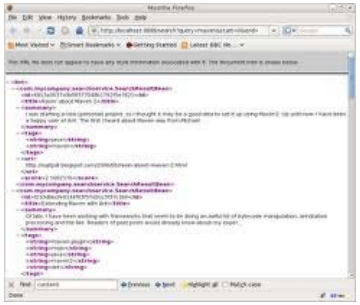
Timeline



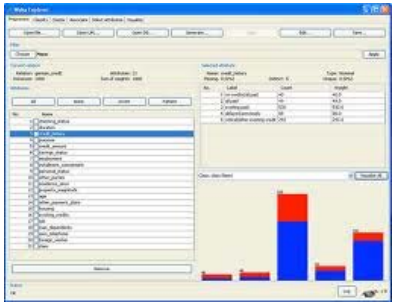
Geo

Search

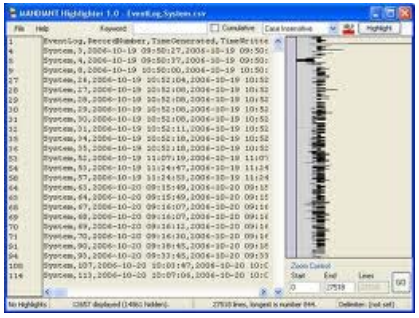
Web Based



Data Mining



Stand Alone



MITRE

Silent Hit Example

- User B is POC for MITRE HAM Radio Club.
- User A searches Application for “MITRE HAM Radio Club”.
- Application returns zero results for said search.
  - However results actually exist
- Application then notifies User B about Users A’s search.
- User B then can make decision to let User A to see data about MITRE HAM Radio Club.
- How is this event audited?

Reactive vs. Predictive Analysis

- **Who's asking you to do analysis?**
  - **Internal vs. External**

- **What assumptions are informing your analysis?**
  - **Strong assumption of innocence; or**
  - **Investigation based off some other predication.**

Maturity of Analysis

- Triage of investigation requests.

- Ad hoc investigations.

- Defined policies/procedures for investigations.
  - Tiered process?
  - Appropriate oversight.

Low Hanging Fruit

- A model program will only focus on advanced analytics once simple analytics are in place.
- Examples of simple analytics:
  - After hours printing
  - Removable media usage
  - Emailing bad actors

Analytical Methods

- Machine Learning Models
- Trending
- Personnel Security Comparison
- Correlative Indicators
- Binary Indicators
- HUMINT/Tip-offs

Understand Business Context

- A model program will collect enough information surrounding an event for later analysis.
- This improves the understanding of why an event occurred and our subjects' intent.
- Focused observation after the fact is a poor and reactive approach; rather one should should apply continuous monitoring to enable a more proactive approach.

Patterns of Behavior

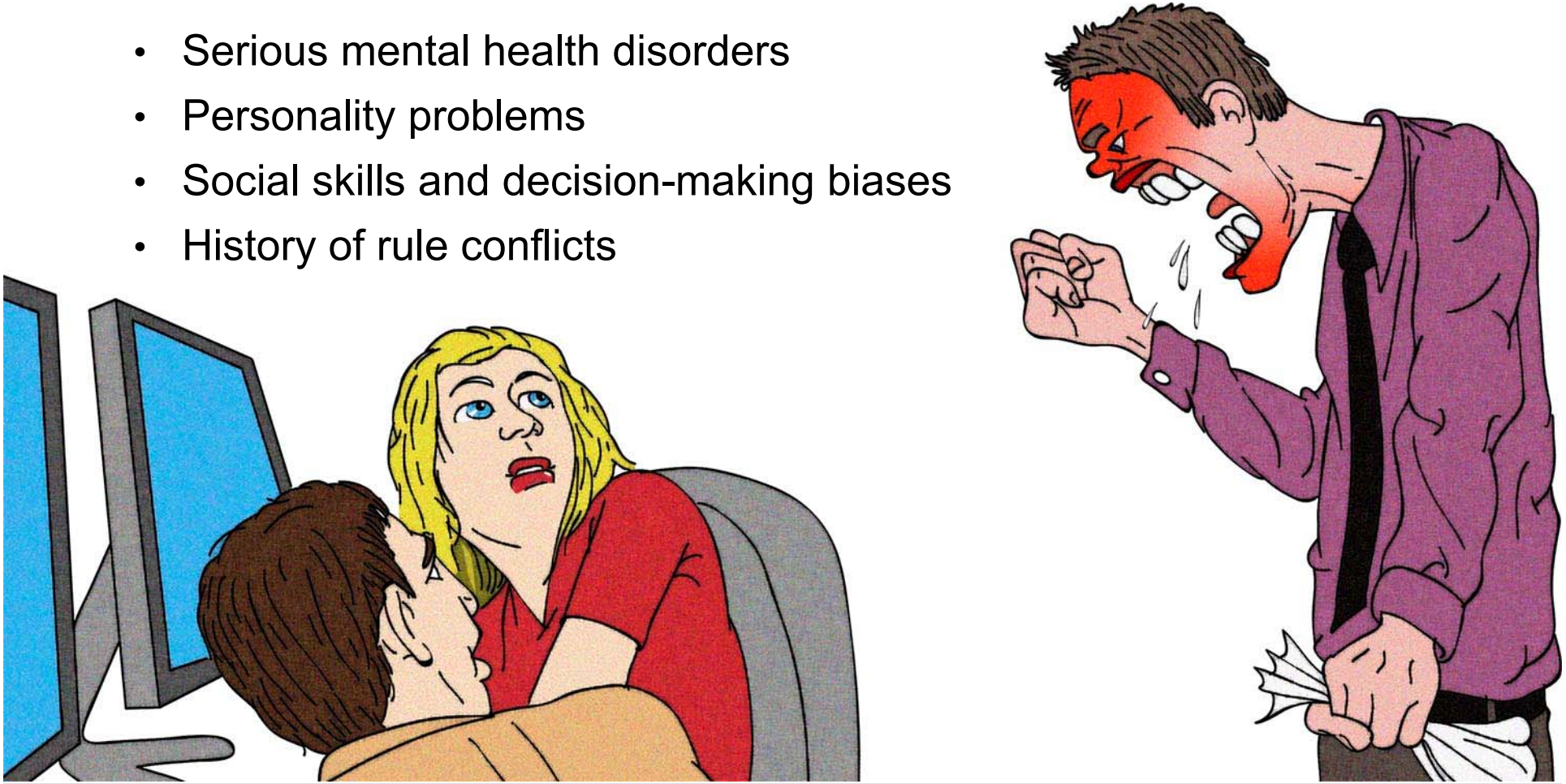
- Insider threat programs are also employing techniques to identify insiders based on proactively identifying patterns of behavior.
- These techniques could employ sophisticated machine learning methods and may result in threat assessments and possibly proactive investigations.

Potential Behavioral Precursors

Personal Predispositions

Predisposition – characteristics of the individual that can contribute to the risk of behaviors leading to malicious activity.

- Serious mental health disorders
- Personality problems
- Social skills and decision-making biases
- History of rule conflicts



Serious Mental Health Disorders

A diagnosed mental health problem for which treatment was recommended or sought

Examples

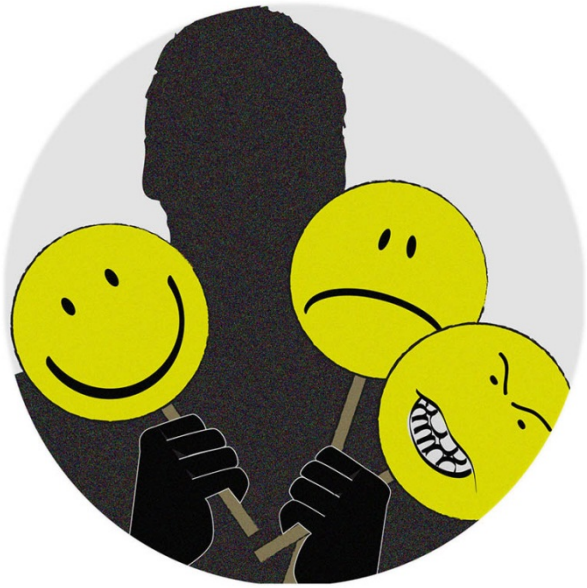
- treated with anti-anxiety and anti-depressant medications prior to the incident
- suffered from alcohol and drug addiction
- suffered from panic attacks
- forced to leave a business partnership due to drug addiction
- reported seeing a psychologist for stress-related treatment prior to the incident
- had a history of physical spouse abuse

Personality Problems

Biased views of self and others that cause maladaptive relations

Examples

- sensitivity to criticism & need for attention
- chronic frustration & feeling unappreciated
- difficulties controlling anger with bursts of inappropriate temper
- chronic sense of victimization or mistreatment
- chronic grudges against others
- grandiose/above the rules
- subject is avoided by others or they “walk on eggshells” around him or her
- bragging, bullying, spending on fantasy-related items
- lack of conscience, impulse control, empathy for others, social impact



Social Skills and Decision-Making Biases

Chronic withdrawal or conflicts with fellow workers, supervisors and security personnel

Examples

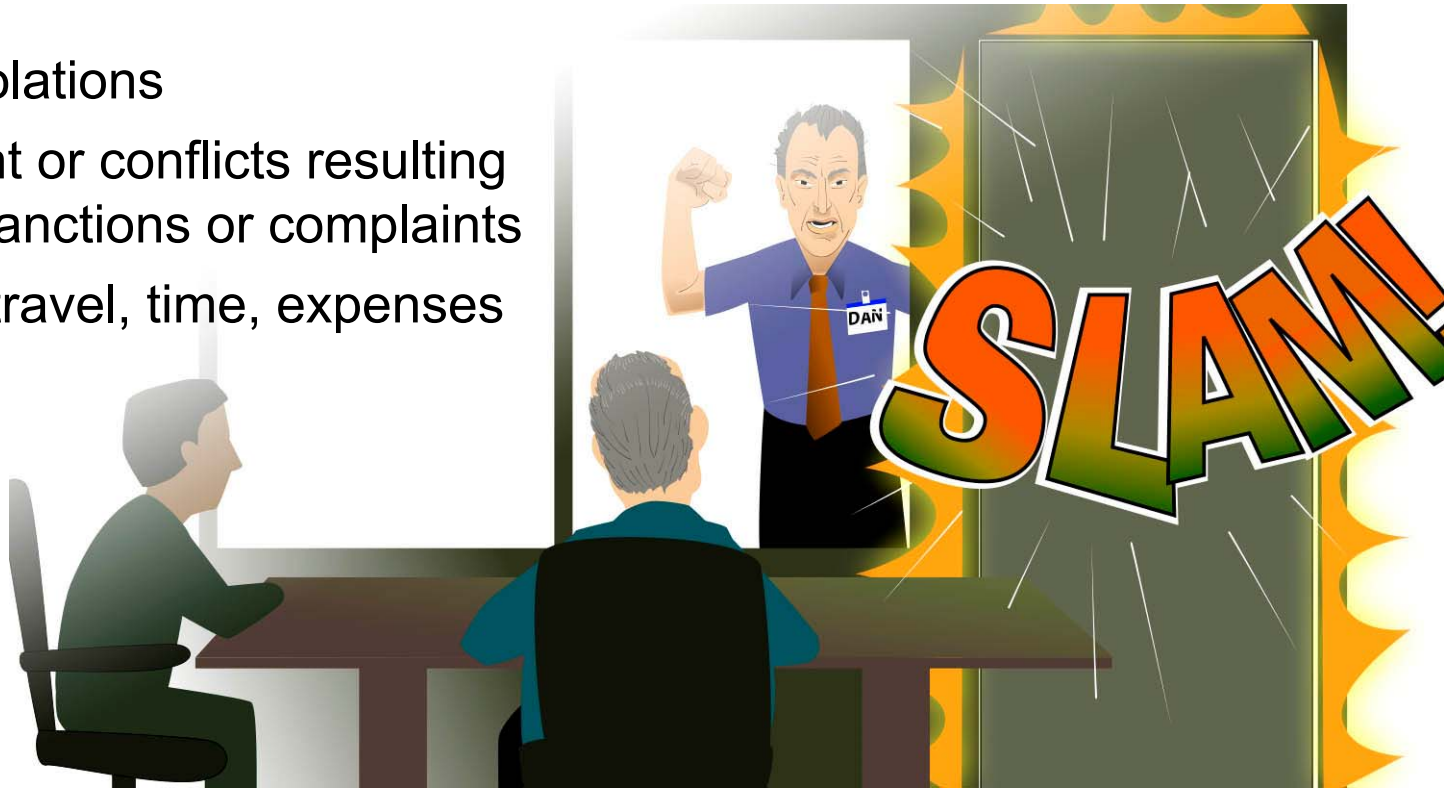
- bullying and intimidation of fellow workers
- refusal to confront supervisors with legitimate work-related complaints due to shyness while complaining to competitors
- serious personality conflicts
- unprofessional behavior
- personal hygiene problems
- inability to conform to rules

History of Rule Violations

Past legal, security, or procedural violations

Examples

- arrests
- hacking
- security violations
- harassment or conflicts resulting in official sanctions or complaints
- misuse of travel, time, expenses



Unmet Expectations Observed in Cases

Salary/bonus

Promotion

Freedom of on line actions

Work ethic

Project requirements - deadlines, milestones

Overestimated abilities

Access to information following termination

Use of company resources

Job dissatisfaction

Supervisor demands

Coworker relations

Responsibilities

Stressors / Sanctions Observed in Cases

TERMINATION

- gross insubordination
- violation of company rules
- poor performance
- not being a team player
- close to Christmas
- false information on background check
- discussion about termination of employment

PASSED OVER FOR PROMOTION

DEMOTION

- due to poor performance
- due to project completion

SANCTIONS

- reprimands for work-related issues
- reprimands for aggressive and malicious behavior
- suspension for excessive absenteeism

TRANSFER BETWEEN DEPARTMENTS

SUPERVISOR

- new supervisor hired
- disagreement with supervisor

ACCESS CHANGED

FINANCIAL

- disagreement over salary & compensation
- bonuses lower than expected
- failure of offering of severance package

DEATH IN FAMILY

DIVORCE

EXPLOSIVE DISAGREEMENT WITH COLLEAGUES

TERMINATION OF SUBCONTRACTOR CONTRACT

TERMINATION OF PARTNERSHIP BECAUSE OF MONEY

CO-WORKERS OVERRIDING DECISIONS

RESPONSIBILITIES REMOVED FROM PROJECTS

OUTSOURCING OF PROJECT

SUSPENSION OF INTERNET ACCESS

Behavioral Precursors Observed in Cases

Drug use

Conflicts (coworkers, supervisor)

Aggressive or violent behavior

Web surfing, chat rooms at work

Mood swings

Bizarre behavior

Used organization's computers for personal business

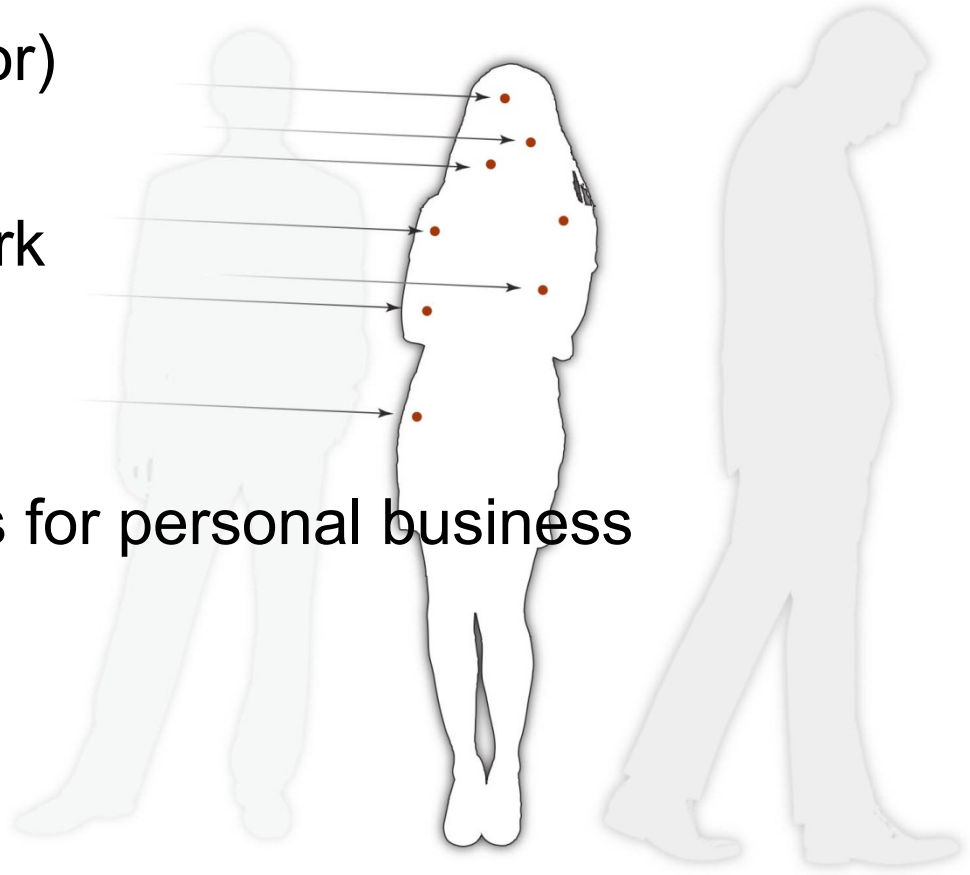
Poor performance

EEO complaint

Absence/tardiness

Sexual harassment

Poor hygiene



Potential Technical Precursors

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 of system logs & removal of history files.

Technical Precursors Undetected in Cases

Downloading and use of “hacker tools” such as rootkits, password sniffers, or password crackers

Failure to create backups as required

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

Refusal to swipe badge to record physical access

Access of web sites prohibited by acceptable use policy

Refusal to return laptop upon termination

Use of backdoor accounts

Use of organization’s system for game playing, violating acceptable use policy

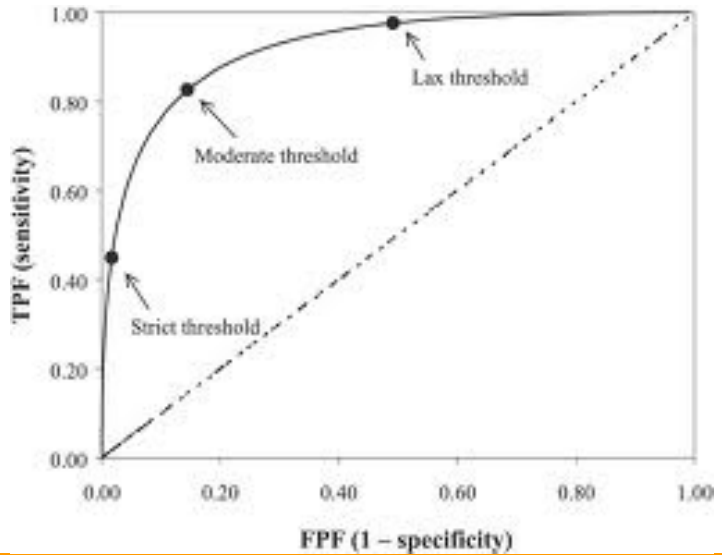
Set up every new computer so he could access it remotely

Program Evaluation

MITRE

Program Validation

- One needs to continually assess a program's capability areas to improve and optimize performance.
  - Metrics for data source Integration
    - Maturity of data source 1 to 5 scale
  - Analysis techniques
    - No ground truth
    - Measurement of false positives and false negatives over sliding window of time
  - Investigative outcomes
    - Metrics
- Procedures should reflect continual validation.



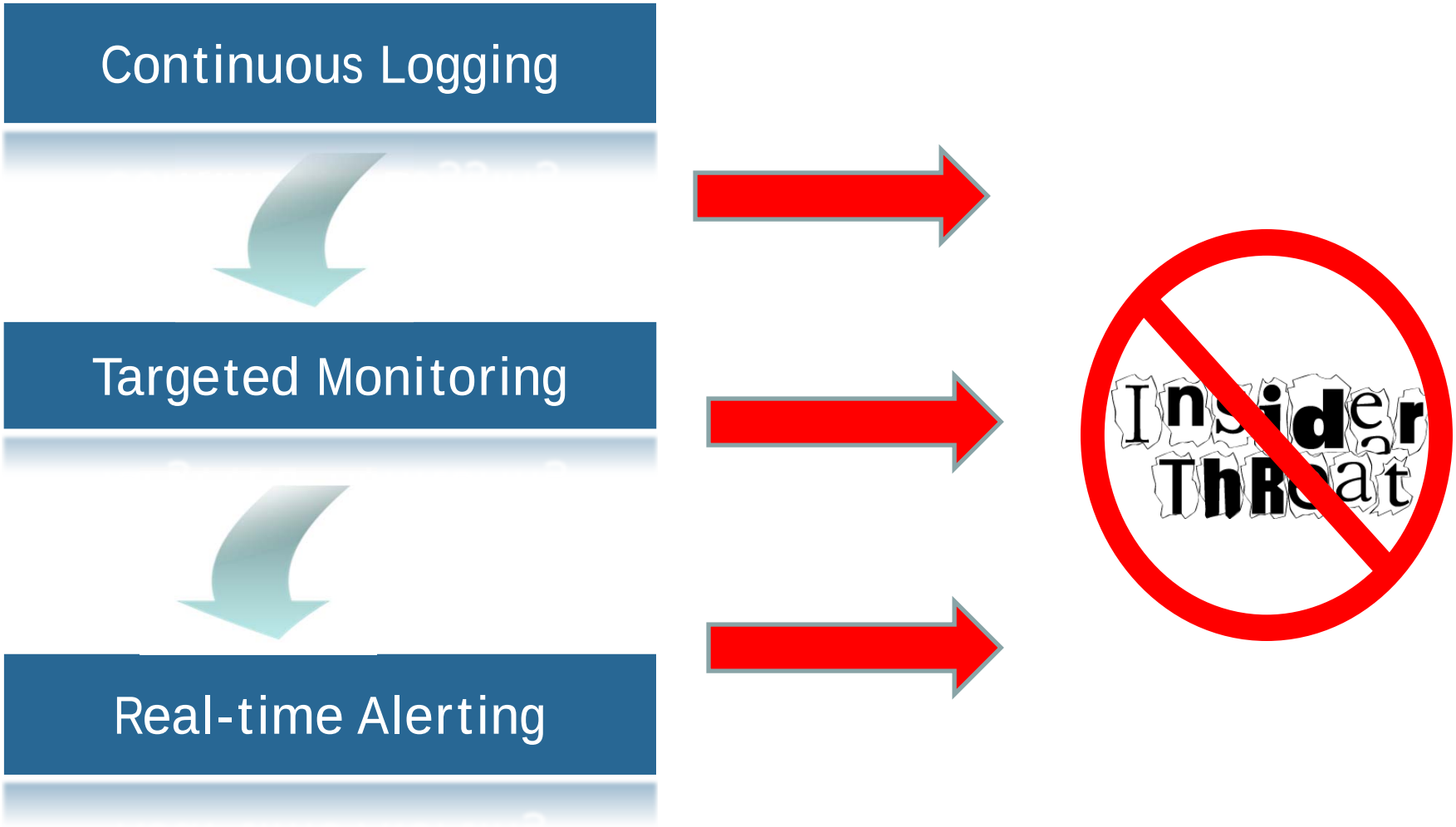
MITRE

Assessing an Insider Threat Program

- Is a program working?
  - How can you tell?
- Is the program big enough?
  - What is the right measure?
- Where should we invest to better a program?
  - Did it work?

Risk Mitigation Strategies

Our Suggestion



Short Term

1. Form an insider threat team that includes HR, Legal, IT, Information Security, Data Owners, Management, Security
2. Create policies that cross organizational boundaries – work with legal counsel
3. Consistently enforce the policies
4. Develop processes and implement controls that enforce communication across departments

Long Term

Automated detection mechanism

- Unified rules engine configured with insider threat indicators and risk thresholds
- Data mining system that correlates unstructured data contained in logs, browsing information, email, internal documents, performance reviews, physical access, etc.
- Intelligent reasoning system that can make a decision about whether to flag a user as being a risk to the organization.

Summary of Practices in Common Sense Guide

Consider threats from insiders and business partners in enterprise-wide risk assessments.	Consider insider threats in the software development life cycle.
Clearly document and consistently enforce policies and controls.	Use extra caution with system administrators and technical or privileged users.
Institute periodic security awareness training for all employees.	Implement system change controls.
Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.	Log, monitor, and audit employee online actions.
Anticipate and manage negative workplace issues.	Use layered defense against remote attacks.
Track and secure the physical environment.	Deactivate computer access following termination.
Implement strict password and account management policies and practices.	Implement secure backup and recovery processes.
Enforce separation of duties and least privilege.	Develop an insider incident response plan.

Clear Escalation Path

- Once an incident occurs, there should be an established escalation plan for all involved parties
  - Established leads
  - Responsible parties for network response
  - Law Enforcement/Counter Intelligence involvement
- Coordinate response
  - CND operates network controls
  - LE/CI approaches subject
  - Security/CND performs damage assessment

- Programs need to have the technical capability to separate and isolate event data for investigative or prosecutorial reasons.

MITRE

Actions to take?

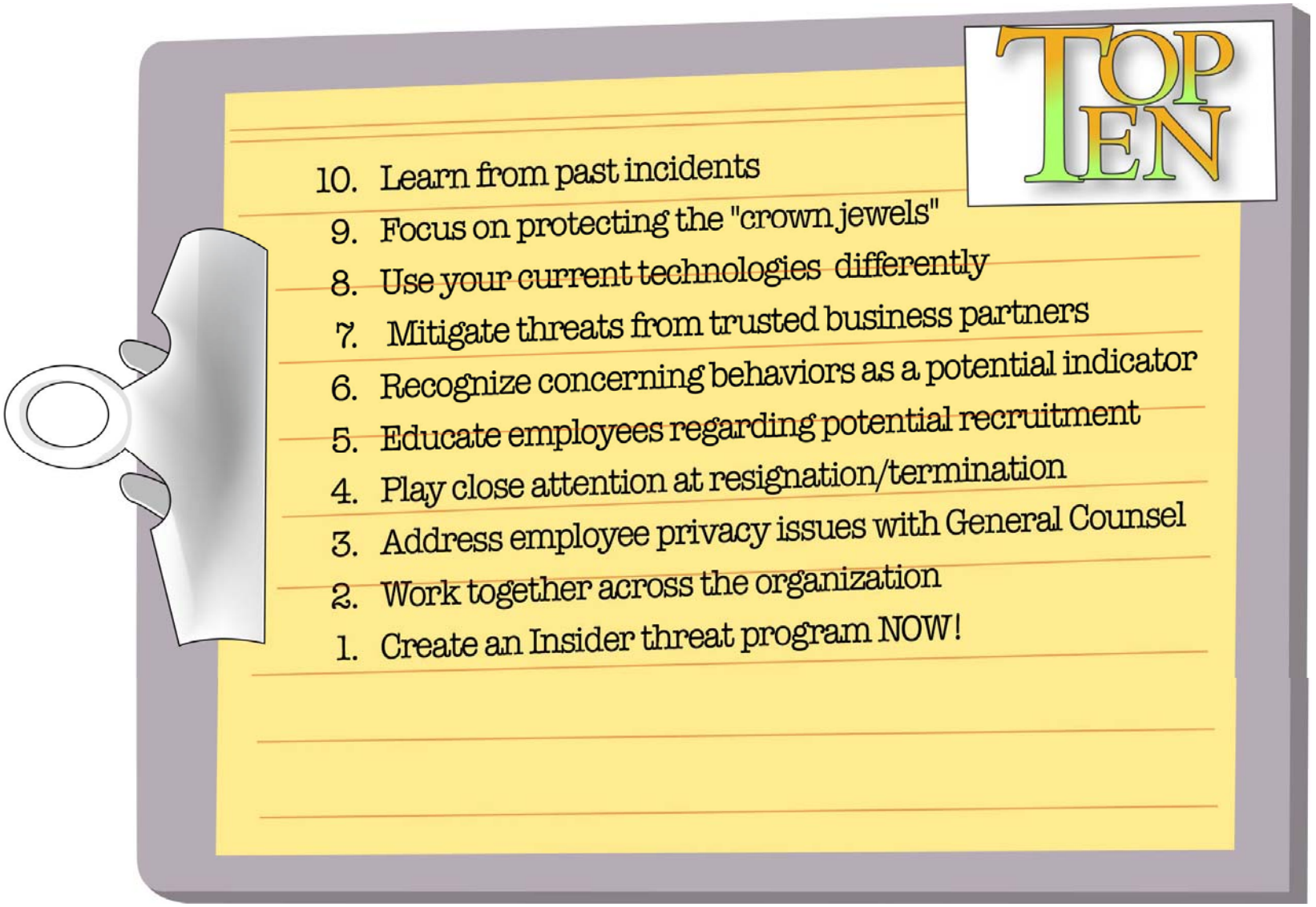
- Deny access to resource

- Escalate surveillance

- Contact authorities

Best Practices

The CERT Top 10 List for Winning the Battle Against Insider Threats



Program Best Practices Summary (1/3)

- Policy
  - Have organizational audit policy establishing responsibilities
  - Issue rules of behavior and banners
  - Properly deal with privacy information
- Authority
  - Immediate notification of FBI for non-DoD entities
- Prevention
  - Apply DLP to all systems in all enclaves

Program Best Practices Summary (2/3)

- **Collection**
  - Focus on Cyber observables
  - InT included in mature auditing program
  - Collect and merge disparate data sources
  - Supply integration guidance to organization
  - Apply continuous monitoring
  - Understand business context
- **Personnel Review**
  - Collected information should be stored for a considerable amount of time
- **Threat Awareness**
  - Involve CI as part of continuous monitoring

Program Best Practices Summary (3/3)

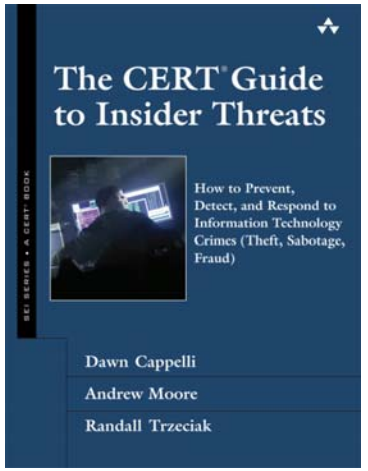
- **Analysis**
  - Use past Insider activity for new indicators
  - Focus on “low-hanging” fruit first, increase sophistication
  - Continually validate analytical processes
- **Attribution**
  - Solid attribution for all events
  - Bound events and attribution information with start and end times.
- **Incident Response**
  - Bounded process for tiered triage
  - Establish clear escalation path
- **Investigation**
  - Perform both “reactive” and “proactive” investigations

Resources

CERT Resources

Insider Threat Center website (http://www.cert.org/insider_threat/)

Common Sense Guide to Prevention and Detection of Insider Threats (http://www.cert.org/archive/pdf/CSG-V3.pdf)



Insider threat workshops

Insider threat assessments

New controls from CERT Insider Threat Lab

Insider threat exercises

The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (SEI Series in Software Engineering) by Dawn M. Cappelli, Andrew P. Moore and Randall F. Trzeciak

MITRE Resources

ELICIT: A system for detecting insider who violate need-to-know

http://www.mitre.org/work/tech_transfer/technologies.html

Insider Threats: Countering Cyber Crime from Within

http://www.mitre.org/news/digest/homeland_security/10_09/cyber_crime.html

Human Behavior, Insider Threat, and Awareness: An Empirical Study of Insider Threat Behavior

http://www.mitre.org/work/tech_papers/2010/09_3130/

Insider Threat Program: Best Practices

by Mark Guido and Marc Brooks

Contact Information

Randall F. Trzeciak
Technical Team Lead, CERT Insider Threat Center
CERT Program, Software Engineering Institute
+1 412 268-7040 – Phone
rft@cert.org – Email

Robin M. Ruefle
Technical Team Lead, ETVM Organizational Solutions
CERT Program, Software Engineering Institute
+1 412 268-6752 – Phone
rmr@cert.org – Email

Marc W. Brooks
MITRE
+1 703 983-7647 – Phone
mbrooks@mitre.org – Email

Questions?