NISPOM Change 2: Considerations for Building an Effective Insider Threat Program

Randall Trzeciak (rft@cert.org)

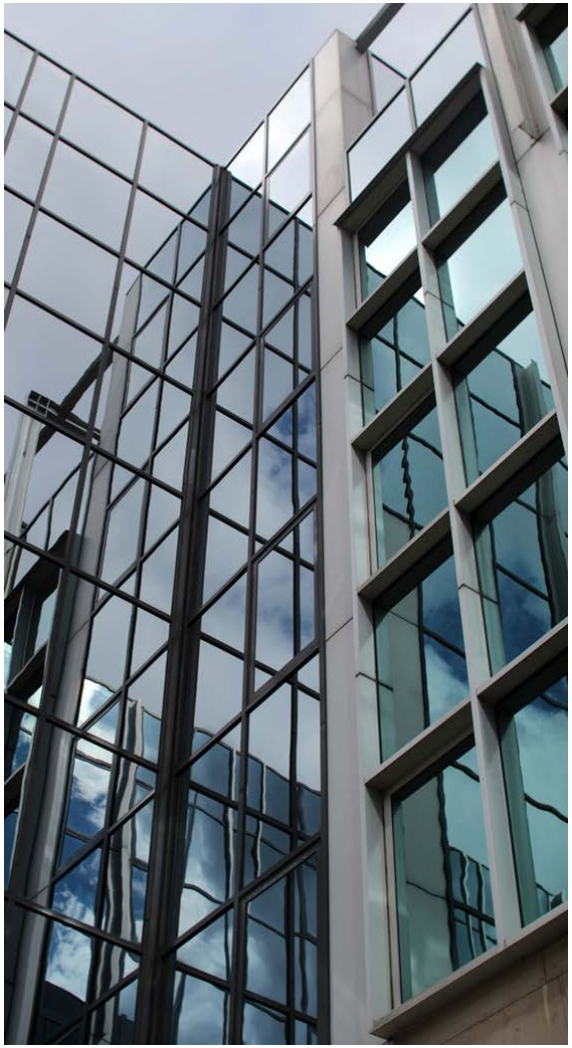
July 7, 2016

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM-0002495

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

Polling Question 2

Would you characterize your organization as:

1. Small (Less than 100 employees)
2. Medium (Between 100 and 999 employees)
3. Large (Between 1000 and 10000 employees)
4. Very Large (Greater than 10000 emplyees)

Executive Order 13587

Executive Order 13587

Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

October 7, 2011

“Our Nation’s security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely.”

Executive Order 13587

"This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals."

Executive Order 13587

"These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and system security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government."

Polling Question 2

Do you currently have an insider threat program in place:

1. Yes
2. No
3. Not Sure

General Responsibilities of Agencies

The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks.

- Designate a senior official to oversee classified information sharing and safeguards
- Implement an insider threat detection and prevention program
  - Consistent with guidance and standards developed by Insider Threat Task Force (ITTF)
- Perform self-assessments of compliance with policies and standards and report results annually to Senior Information Sharing and Safeguarding Steering Committee
- Provide information and access to enable independent assessments

Insider Threat Task Force -1

Interagency Insider Threat Task Force

- Co-chaired by the Attorney General and Director of National Intelligence
  - Officers from DoS, Defense, Justice, Energy, Homeland Security, ODNI, CIA, FBI, ONCIX

- Develop a government-wide insider threat program
  - Deter, detect, and mitigate insider threats
  - Safeguard classified information
  - Develop policies, objectives, and priorities

Insider Threat Task Force -2

Responsibilities

- Develop government-wide policy for deterrence, detection, and mitigation of insider threats
- Develop minimum standards and guidance for implementation of the insider threat program
- Yearly: add or modify minimum standards and guidance, as appropriate
- Conduct independent assessments of adequacy of insider threat programs
- Provide assistance to agencies and dissemination of best practices

National Insider Threat Policy -1

"The E.O. directs the ITTF to assist agencies in developing and implementing their insider threat programs, while ensuring the program standards do not erode civil liberties, civil rights, or privacy protections for government employees."

- Issued in November 2012

National Insider Threat Policy -2

"Directs executive branch departments and agencies to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect classified national security information"

- Applicable to all D&As with access to classified information, or that operate or access classified computer networks;
- All employees with access to classified information or networks

NISPOM Change 2 -1

National Industrial Security Program Operating Manual Change 2

Published May 18, 2016

Requires contractors* to establish and maintain an insider threat program to detect, deter, and mitigate insider threats.

Insider Threat Industrial Security Letter :

"gather, integrate, and report relevant and credible information covered by any of the 13 personnel security adjudicative guidelines that is indicative of a potential or actual insider threat to deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risk of an insider threat."

* Contractor: any industrial, educational, commercial, or other entity that has been granted a facility security clearance (FCL) by a Cognizant Security Agency (CSA)

NISPOM Change 2 -2

Insider Threat Program

- The contractor will establish and maintain an insider threat program
  - Gather, integrate, and report relevant and available information indicative of a potential or actual insider threat
  - In accordance with E.O. 13587
- The contractor will designate a U.S. citizen employee
  - Senior official and cleared with the FCL Office
  - To establish and execute an insider threat program

NISPOM Change 2 -3

Insider Threat Training

- Ensure that contractor program personnel assigned insider threat program responsibilities and all other cleared employees are trained.
- Must be trained in:
  - Counterintelligence and security fundamentals
  - Procedures for conducting insider threat response actions
  - Applicable laws and regulations regarding gathering, integration, retention, safeguarding, and use of records and data (including consequences of misuse of data)
  - Applicable legal, civil liberties, and privacy policies

NISPOM Change 2 -4

Insider Threat Training

- All cleared employees must be provided insider threat awareness training
  - Either in-person or computer-based
  - Within 30 days of initial employment or prior to being granted access to classified information
  - Annually

Polling Question 4

Do you anticipate utilizing a “full-time” insider threat program team or a part-time program team?

1. Full-Time
2. Part-Time
3. Combination of Both Full and Part Time Staff

What This Means to Contractors

CONTRACTORS MUST HAVE A WRITTEN PLAN IN PLACE TO BEGIN IMPLEMENTING INSIDER THREAT REQUIREMENTS NO LATER THAN NOVEMBER 30, 2016

Insider Threat Program Requirements -1

- Assign an insider threat program (ITP) senior official

- Establish and maintain an ITP to gather, integrate, and report information (from HR, Security, Information Assurance, Legal, counterintelligence) about a potential or actual insider threat.

- Establish procedures to access, share, identify, and collaborate across the contractor organization to report information related to the 13 personnel security adjudicative guidelines. (Contractors are required to report relevant and credible information regarding potential and actual insider threats.)

- Ensure that insider threat programs address all cleared facility locations owned and operated by the contractor.

Insider Threat Program Requirements -2

- Perform yearly self-inspections and certify with DSS.
- Allow independent assessments of their ITP.
- Develop a system or process to identify and report patterns of negligence and carelessness in handling classified information.
- Ensure that insider threat training is provided to all members of the contractor's ITP team and that new ITP team members complete the training within 30 days of joining the program team.

Insider Threat Program Requirements -3

- Require insider threat awareness training for all employees before they are granted access to classified information and refresh their training yearly afterwards. To confirm training is complete, the contractor must have in place a training records management system.

- Implement the DSS-provided information security controls on classified information systems to detect insider threat behavior.

- Establish an oversight mechanism to ensure the proper handling and use of information collected through the ITP.

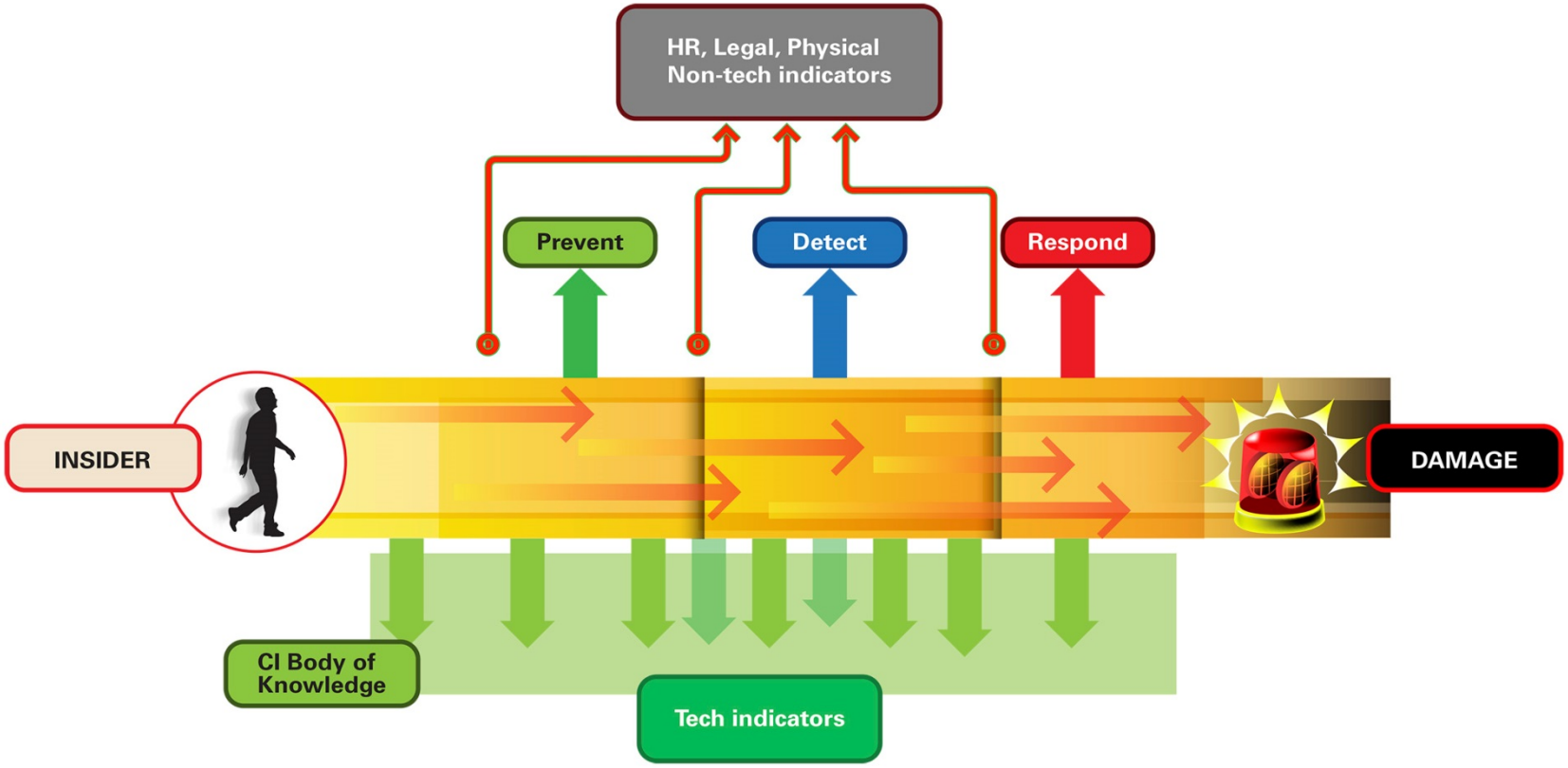
Insider Threat Program Requirements -4

- Establish procedures and processes for insider threat response actions.

- Develop a process to document each insider inquiry, investigation, and remediation.

Goal for an Insider Threat Program

Goal for an Insider Threat Program



Opportunities for prevention, detection, and response for an insider

CERT's Recommendations for Building an Insider Threat Program

Anomaly Detection

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

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

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.

Behavioral Data

Behavioral Data Sources

Human Resources Management System Data

Help Desk Trouble Ticket System Logs

Physical Access Logs

Phone Logs

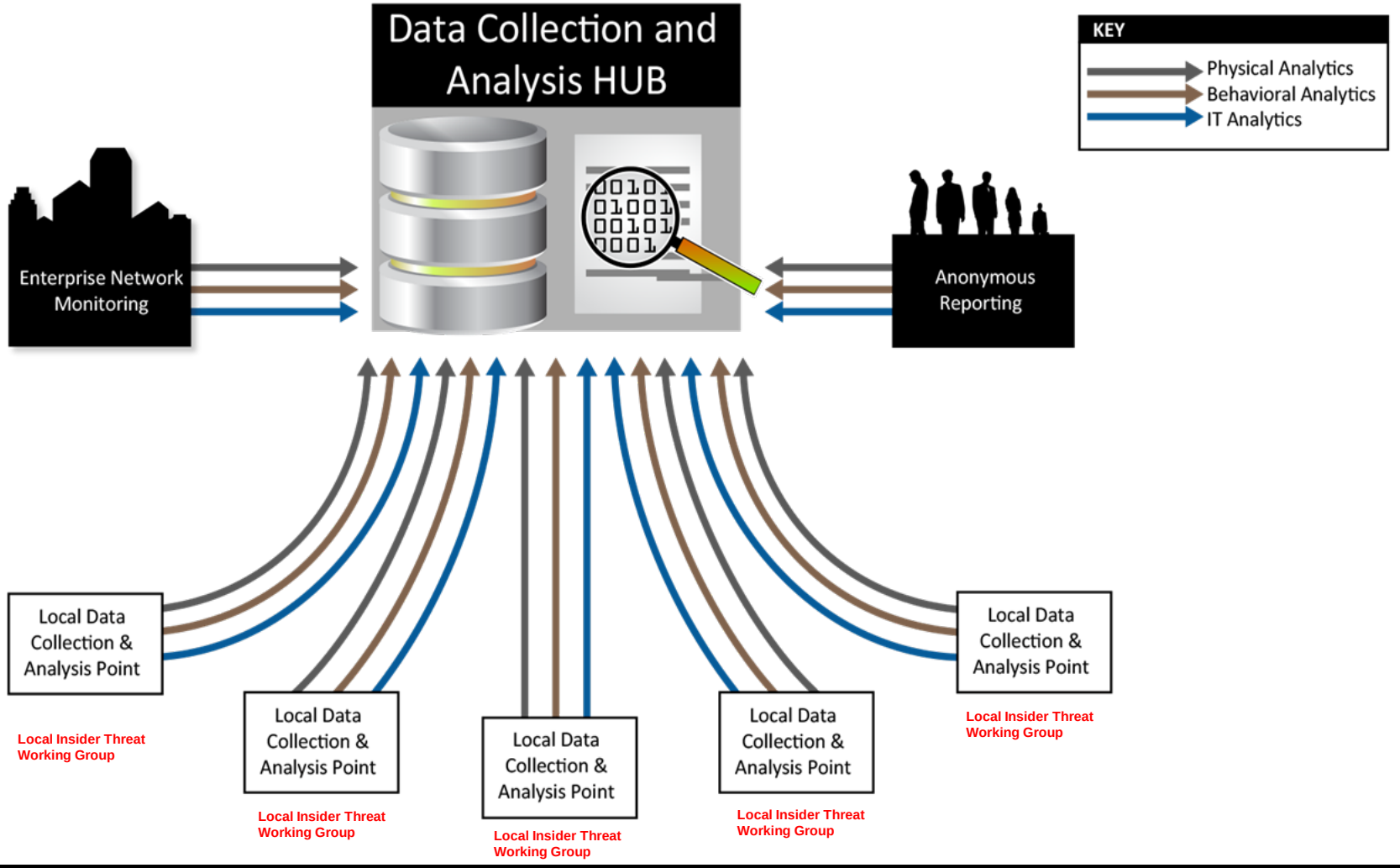
Personnel Security Systems

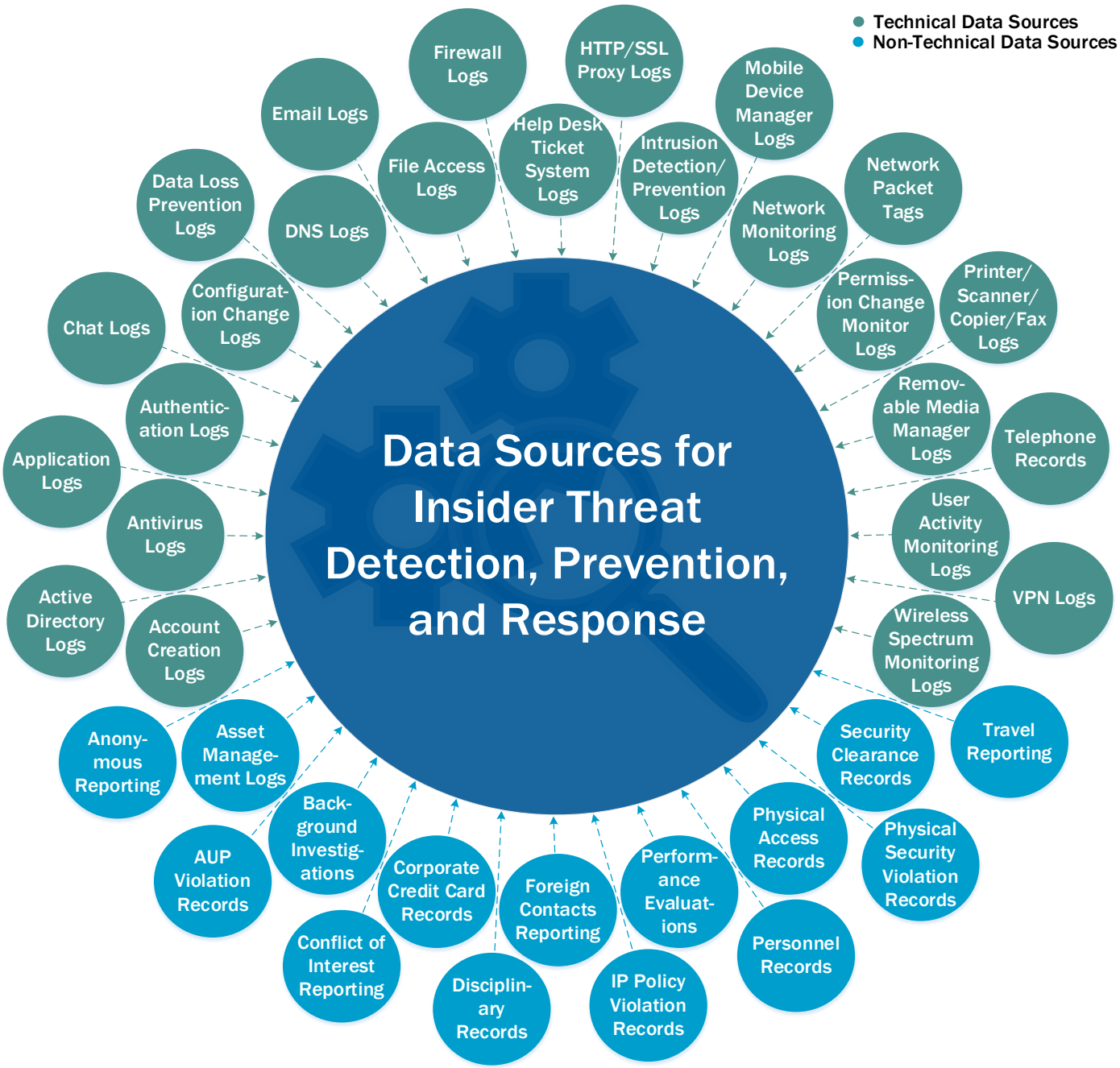
Foreign Travel and Reporting Systems

Financial Systems

Creation of a Data Analytic Hub

HUB Data Collection – Notational





Best Practices: Common Sense Guide to Mitigating Insider Threats

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017

CERT Recommended Best Practices for Insider Threat Mitigation

Consider threats from insiders and business partners in enterprise-wide risk assessments.	Institutionalize system change controls.
Clearly document and consistently enforce policies and controls.	Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
Incorporate insider threat awareness into periodic security training for all employees.	Monitor and control remote access from all end points, including mobile devices.
Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	Develop a comprehensive employee termination procedure.
Anticipate and manage negative issues in the work environment.	Implement secure backup and recovery processes.
Know your assets.	Develop a formalized insider threat program.
Implement strict password and account management policies and practices.	Establish a baseline of normal network device behavior.
Enforce separation of duties and least privilege.	Be especially vigilant regarding social media.
Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.	Close the doors to unauthorized data exfiltration.
Institute stringent access controls and monitoring policies on privileged users.	

Wrap Up

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/

References -1

Executive Order 13587: Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

National Insider Threat Policy

https://www.ncsc.gov/nittf/docs/National_Insider_Threat_Policy.pdf

References -2

DoD 5220.22-M: National Industrial Security Program Operating Manual
http://www.dss.mil/documents/odaa/nispom2006-5220.pdf

Industry Insider Threat Information and Resources Page (DSS)
http://www.dss.mil/it/index.html

Insider Threat Industrial Security Letter
http://www.dss.mil/documents/isp/ISL2016-02.pdf

13 Personnel Security Adjudicative Guidelines
https://www.gpo.gov/fdsys/pkg/CFR-2012-title32-vol1/xml/CFR-2012-title32-vol1-part147.xml

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/