Low Cost Technical Solutions to Jump Start an Insider Threat Program

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

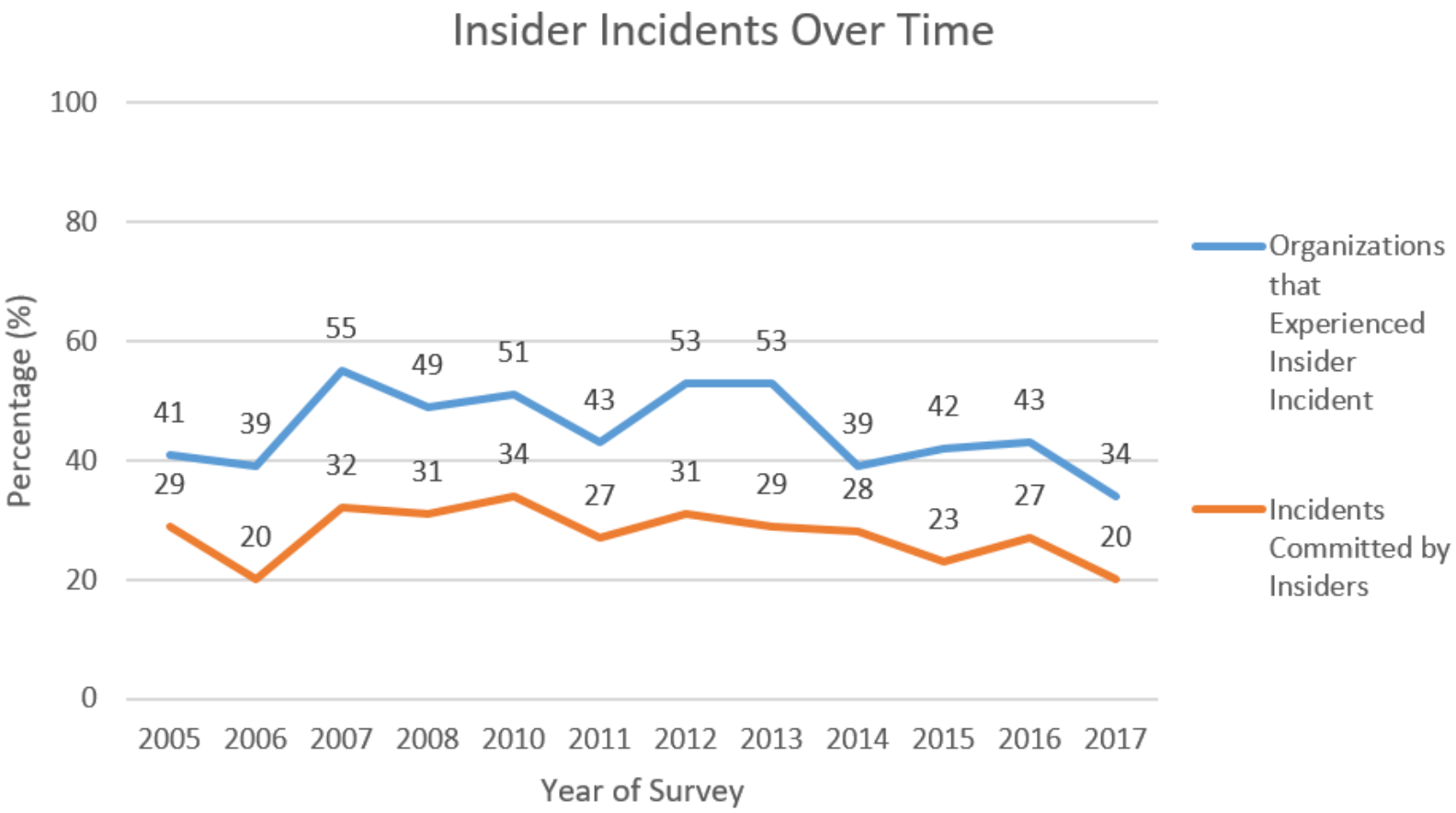
Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0668

Getting Your Program Started

Why start a program? – The Prevalence of Incidents

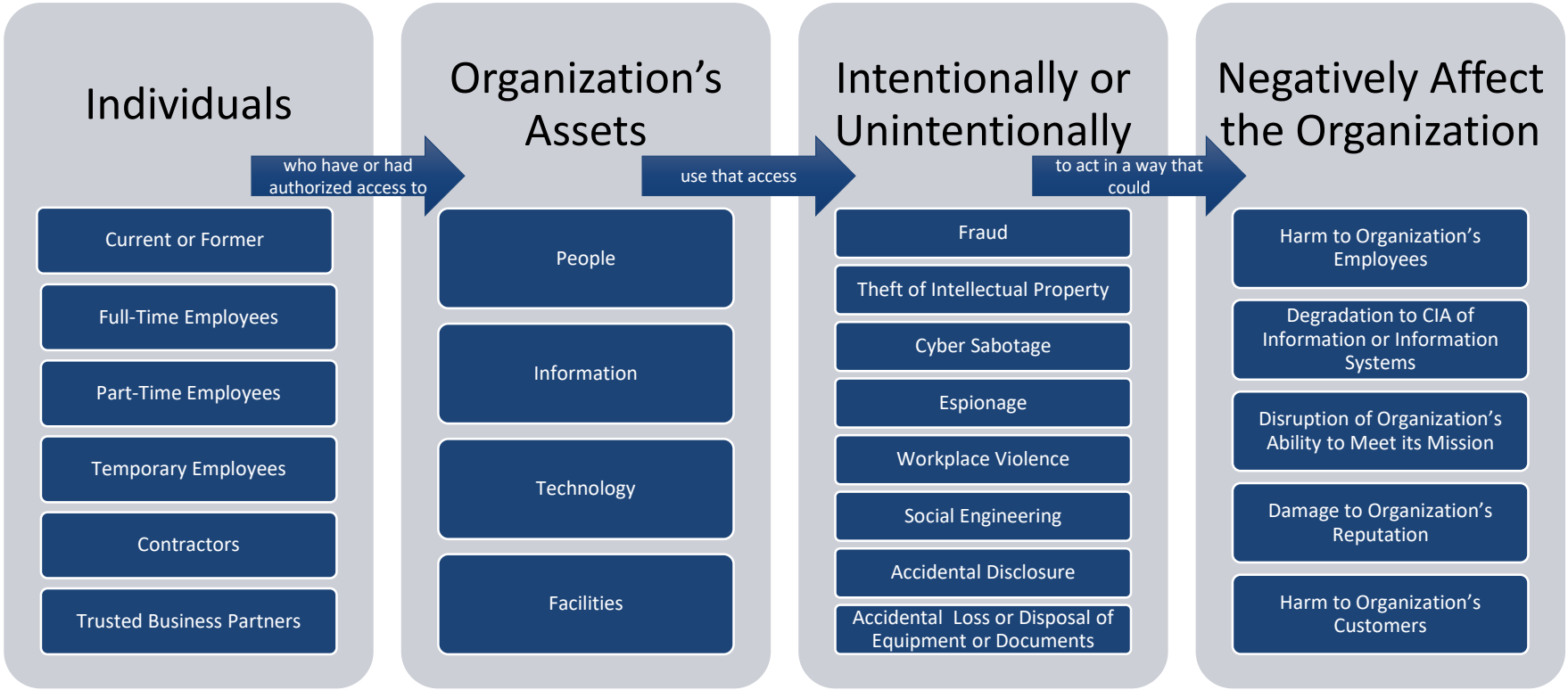


Source: U.S. State of Cybercrime Surveys, 2005-2017, CSO Magazine, USSS, Carnegie Mellon Software Engineering Institute, Price Waterhouse Cooper, ForcePoint

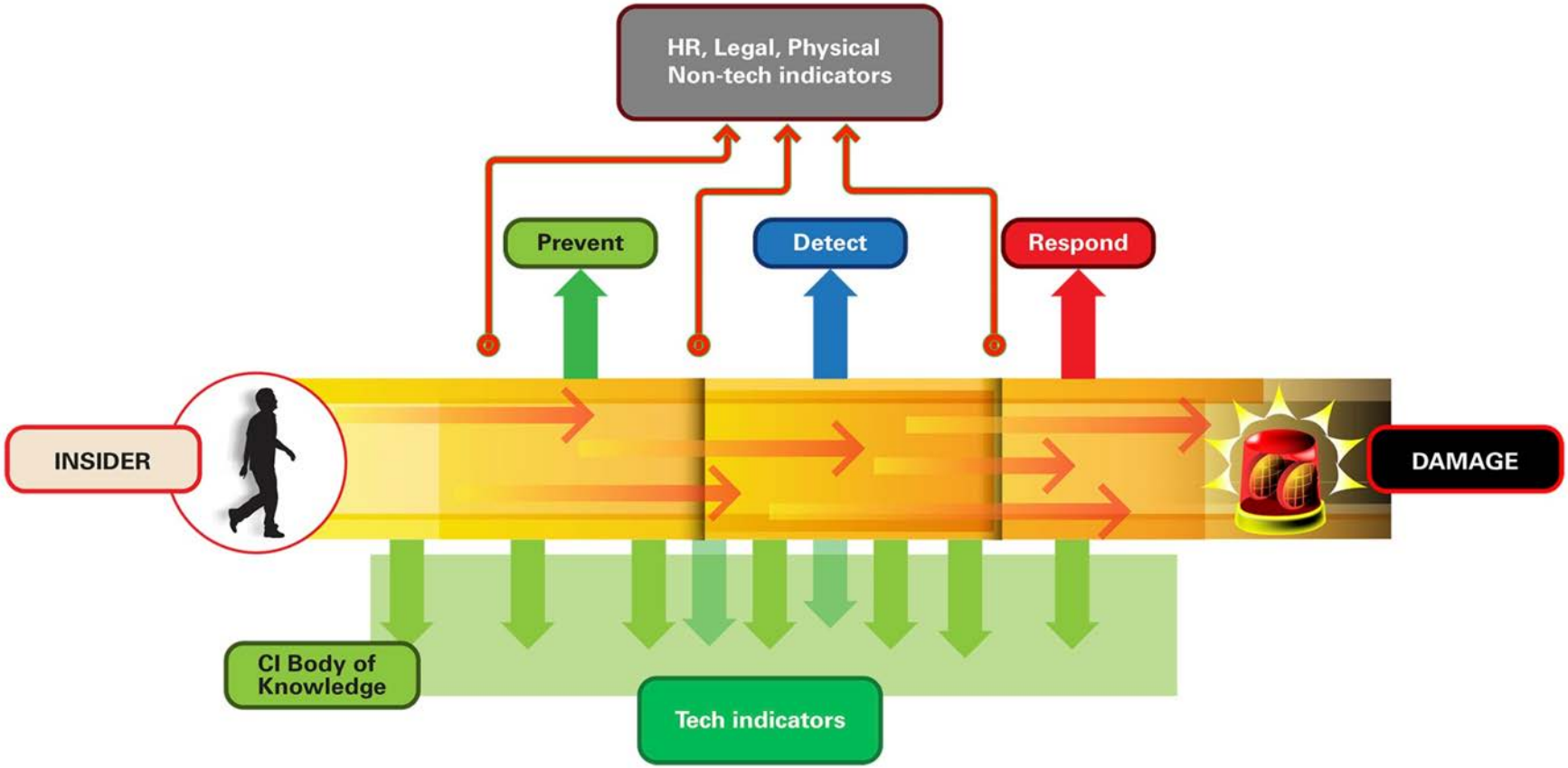
Today's Objectives

- Understand Insider Threat Challenges
- Familiarize you with five high-level tool categories
- Discuss the key features of each tool category
- Discuss the relationship between tools in each category
- Propose low cost tools for each category

Multifaceted Challenge



What are the goals of the program?



Insider Threat Tools Vary In Features and Functions

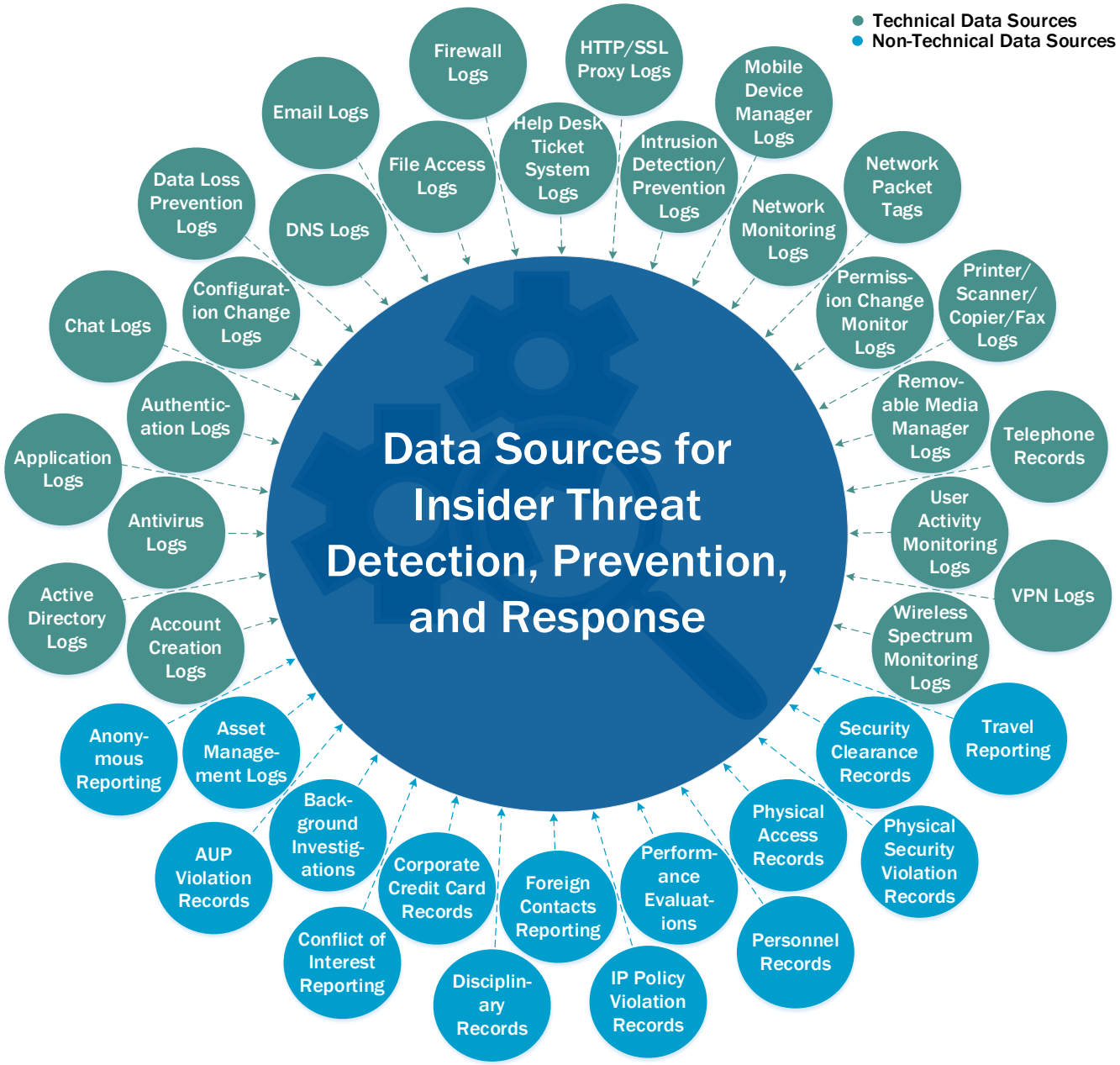
Auditing Host-based Activity	Auditing Network-based Activity	Preventing Data from Leaving Authorized Locations
Preserving Forensic Artifacts	Data Visualization	Rule-Based Alerting
Identity Management / Access Management	Data Correlation / Entity Resolution	Anomaly Detection
Machine Learning	Text Analysis	Risk Scoring
Case / Incident Management	Data Masking / Anonymization	… And More …

Prevent
- Stop something from happening
  - Example: Block a sensitive document from being moved to removable media

Detect
- Figure out that something is happening (or about to happen)
  - Example: Alert security staff of unusual file activity

Deter
- Discourage something from happening
  - Example: Present a dialog that requires a user to acknowledge the organization's removable media policy

Respond
- Address something that happened
  - Example: Forensic analysis of an Insider's system



Tool Categories

User Activity Monitoring

- Observe and monitor what users are doing
- Audit Host and network-based Activities, Rule-Based Alerting

Data Loss Prevention (DLP)

- Observe and monitor data as it moves around networks and repositories
- Prevent Data from Leaving Authorized Locations

Security Information and Event Management (SIEM)

- Collect and normalize relevant logs
- Audit Host and network-based Activities, Data Visualization, Rule-Based Alerting, Data Correlation / Entity Resolution, Anomaly Detection, Machine Learning, Case / Incident Management

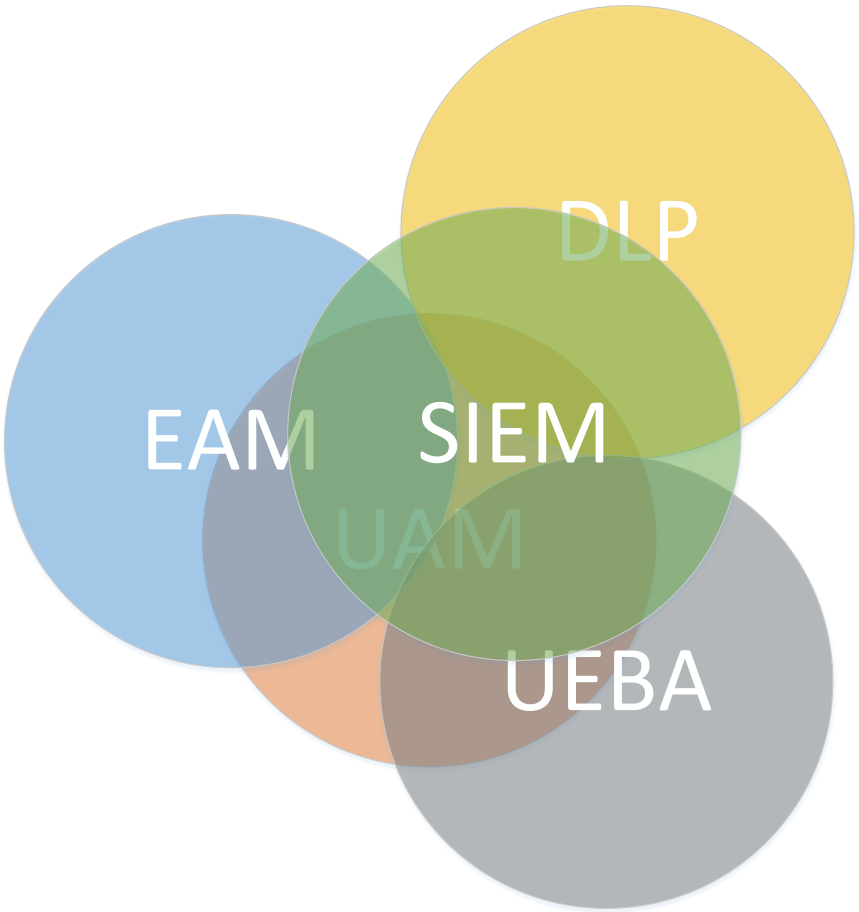
Analytics

- Find anomalies
- Data Visualization, Rule-Based Alerting, Data Correlation / Entity Resolution, Anomaly Detection, Machine Learning, Text Analysis, Risk Scoring, Case / Incident Management, Risk Scoring, Data Masking

Forensics

- Obtain evidence
- Preserving Forensic Artifacts

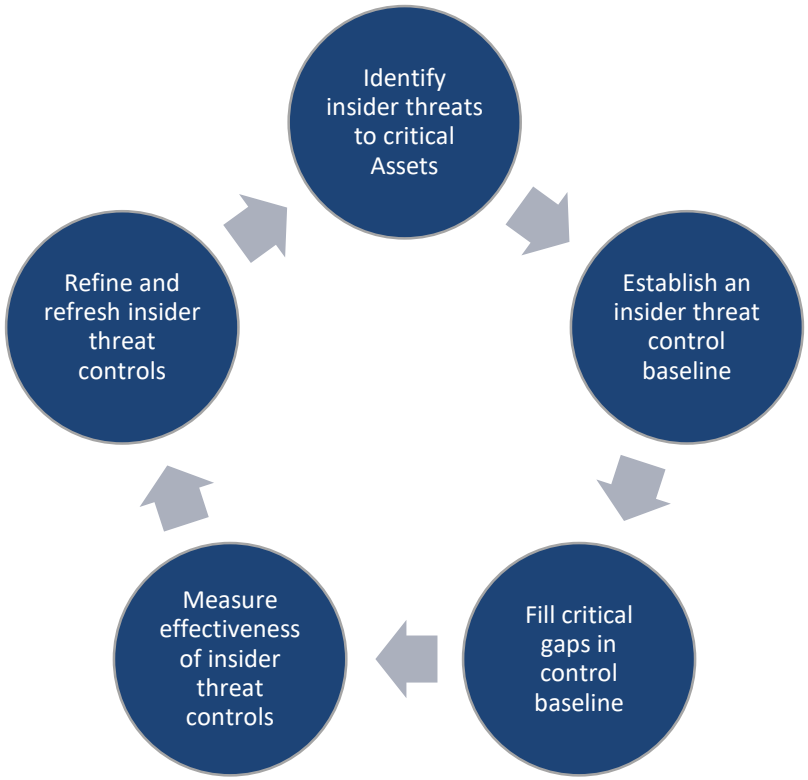
The Insider Threat Tool Landscape



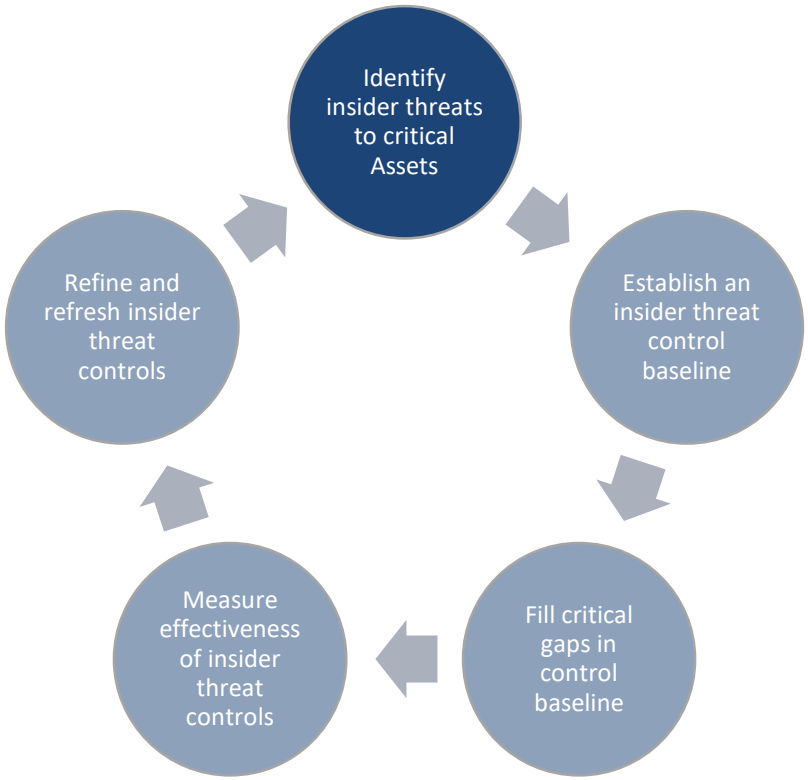
Ongoing effort to understand relationship between capabilities of different types of tools

Fine line between defense in depth and buying the same thing twice

What Can You Do to Implement and Operate Tools?



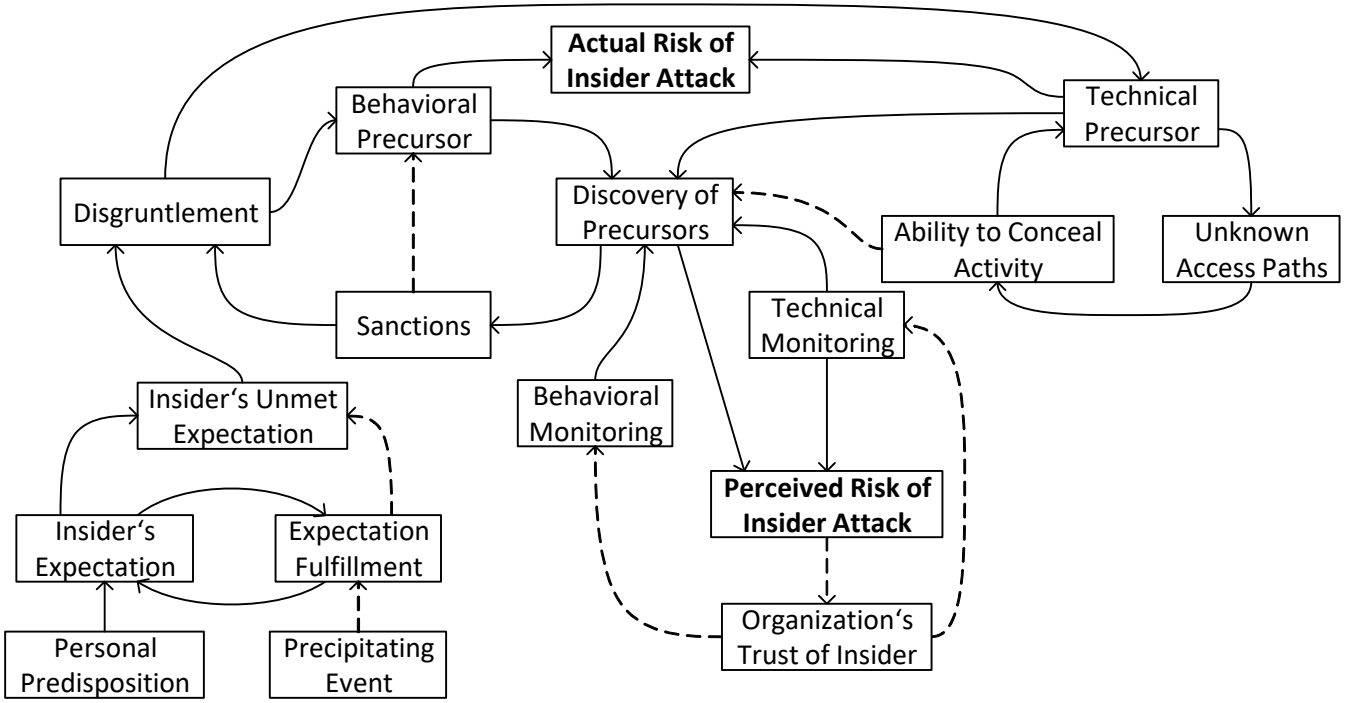
Implementing and Operating Tools



Identifying Risks to Critical Assets

- Enumerate critical assets
  - Get the right stakeholders involved
- Identify risks to those critical assets
  - Use threat modeling to help
  - Different types of threat modeling:
    - PNG
    - Security Cards
    - STRIDE
  - Leverage existing models, like ours!

Sabotage Model



Sabotage Observables

Observable	UAM	DLP	SIEM	Analysis	Forensics
Coworker conflict	X			X	
History of Rule Violation			X	X	
Disgruntlement or unmet expectations (demotion or termination)	X			X	
Creation of unknown access paths (backdoor accounts)	X		X	X	X
Deletion of Logs	X		X	X	X
Introduction of unauthorized code or software	X		X		X

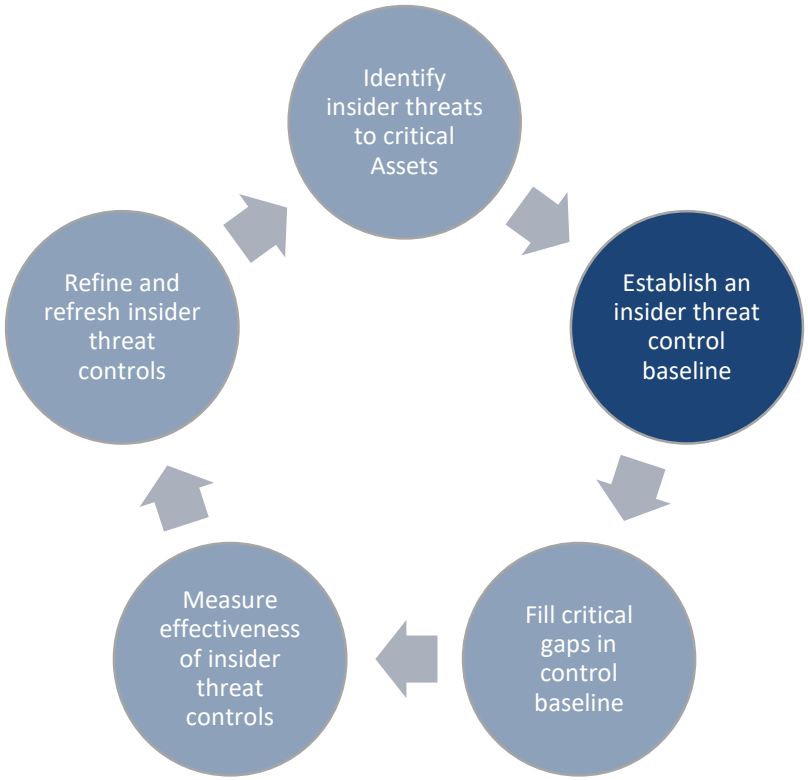
Fraud Observables

Observable	UAM	DLP	SIEM	Analysis	Forensics
Network or Host Data Exfiltration	X	X	X	X	X
Recruitment of insider via chat or email	X		X	X	
Creation or use of fraudulent assets	X		X	X	
Anonymous reporting				X	
Social Engineering	X				
Internal and/or external collusion	X	X			

Theft of Intellectual Property Observables

Observable	UAM	DLP	SIEM	Analysis	Forensics
Network or host data exfiltration	X	X	X	X	X
Physical data exfiltration (print/scan/copy/fax)	X		X		
Announcement of resignation or termination	X				
Access outside of need-to-know	X	X	X	X	
Solicitation from external parties	X	X			
Suspicious travel				X	

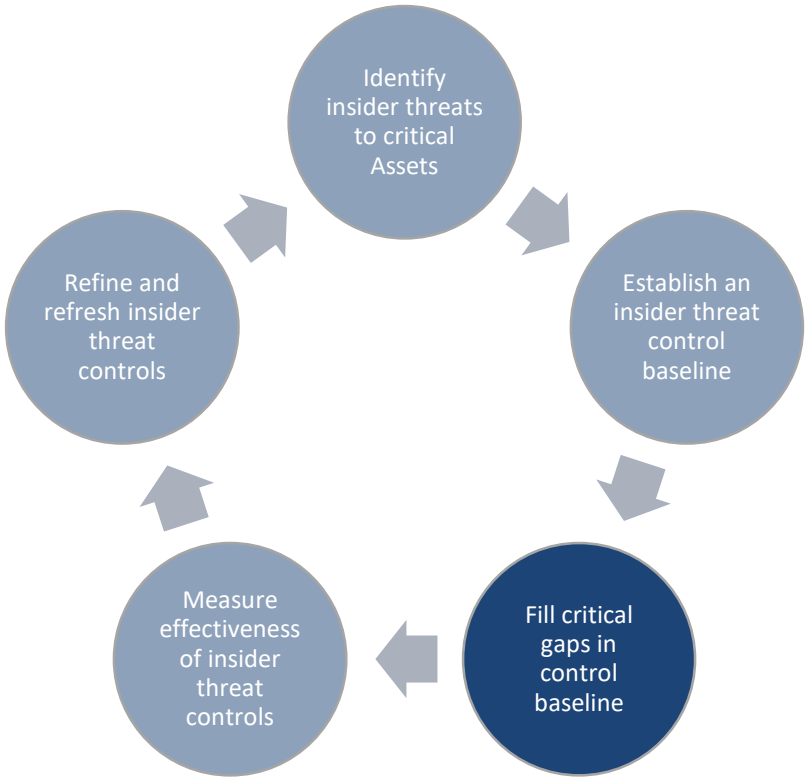
Implementing and Operating Tools



Establish a control baseline

- Start from a solid network foundation that assumes basic capabilities such as:
  - Segmented networking and firewalling
  - Modern operating systems capable of logging
- Enumerate current security controls
  - Technical
  - Physical
  - Administrative
- Understand what you need
  - Standards such as NIST 800-53

Implementing and Operating Tools



User Activity Monitoring

User Activity Monitoring (UAM)

- Host based auditing, monitoring and prevention controls including:
  - Application monitoring
  - File and registry monitoring
- Key functionality includes:
  - rule-based alerts or triggers
  - logging/recording to central analyst interface
- Difficult to achieve comprehensive coverage with low-cost tools

User Activity Monitoring Tools - 1

Open Source HIDS SECurity (OSSEC)

- Host-based Intrusion Detection System
- Provides registry monitoring, file system monitoring, USB device insertion monitoring
- Can also monitor network devices via Syslog
- http://www.ossec.net

Squid Proxy and E2Guardian

- Both packages combined provide content filtering and logging.
- Squid: http://www.squid-cache.org
- Dansguardian > E2Guardian: http://e2guardian.org

User Activity Monitoring Tools - 2

Security Onion

- A Linux distribution with a suite of tools for monitoring network traffic and analyzing endpoint logs.
- https://securityonion.net

Intrusion Detection Systems

- Can be positioned strategically to monitor network traffic of key ingress/egress points.
- Several different software packages available:
  - BroIDS: https://www.bro.org
  - Snort: https://www.snort.org
  - Suricata IDS: http://suricata-ids.org

User Activity Monitoring Tools - 3

Packet Capture

- Capture network traffic that can be used for troubleshooting, incident response, and inquiries.
- Several software packages available:
  - tcpdump: http://www.tcpdump.org/
  - WireShark: https://www.wireshark.org/
  - NetworkMiner:http://www.netresec.com/?page=NetworkMiner

User Activity Monitoring Tools - 4

Operating System Logs

- Windows Event Logs
  - Process and File CRUD auditing
- Unix Audit Daemon (auditd)
  - File CRUD auditing
  - Command line auditing

User Activity Monitoring – Windows Event Logs

Log Source	Event ID	Description	Observables
Security	576	Special privileges assigned to new logon	4.1.1-Privileged Access Abuse
Security	624	User Account Created	4.2.1-Unauthorized Access Path Creation
Security	851	A change has been made to the Windows Firewall application exception list	4.2.1-Unauthorized Access Path Creation
Security	852	A change has been made to the Windows Firewall port exception list	4.2.1-Unauthorized Access Path Creation
Security	857	The Windows Firewall setting to allow remote administration, allowing port TCP 135 and DCOM/RPC, has changed	4.2.1-Unauthorized Access Path Creation
Security	4719	System audit policy was changed	4.8.3-Insider Modified/Deleted Logs/Activity
Security	4720	A user account was created	4.2.1-Unauthorized Access Path Creation
Security	4782	The password hash for an account was accessed	1.2.4-Hacking Related Activities
Security	4797	An attempt was made to query the existence of a blank password for an account	1.2.4-Hacking Related Activities
Security	6416	A new external device was recognized by the system.	3.2.2-Insider Attached External Hardware To Organization Desktop
Microsoft-Windows-DriverFrameworks-UserMode-Operational	2003	Loading drivers to control a newly discovered device.	4.6.2-Data Exfiltration - Removable Media
Microsoft-Windows-PrintService/Operational	310	Microsoft-Windows-PrintSpooler	4.6.1-Data Exfiltration - Paper
Application	1033	MsiInstaller	3.2.1-Unauthorized Software Installation
Microsoft-Windows-Windows Defender/Operational	1006	The antimalware engine found malware or other potentially unwanted software.	4.5.2-Inserted Malicious Code into Operational System
Microsoft-Windows-Windows Defender/Operational	1015	The antimalware platform detected suspicious behavior.	4.5.2-Inserted Malicious Code into Operational System

Data Loss Prevention

Data Loss Prevention (DLP)

- DLP tools allow organizations to control how users interact with and move data across networks and devices
- Key functionality includes monitoring tagged:
  - Data at rest – Disk drives, removable media, backup media
  - Data in motion – network sensors at enclave ingress/egress points
  - Data in use – data movement to removable media
- Generally effective at detecting sensitive information with common formats:
  - Bank Account Numbers, Social Security Numbers, Credit Card Numbers

Data Loss Prevention Tools

OpenDLP (https://github.com/ezarko/opendlp)

- Identification of sensitive data via client/server architecture
  - Scans file systems and databases

MyDLP (http://www.mydlp.com)

- Identification of sensitive data via client/server architecture
  - Client agent detects data moving to removable media and print jobs
  - Squid network proxy detects data moving over HTTP/S
  - Paid enterprise edition adds more functionality, such as file repository scanning

Security Information and Event Management

Security Information and Event Management (SIEM)

- Aggregate and normalize logs into a centralized repository and can perform some level automated analysis on those logs
- Also typically utilized by the Security Operations Center (SOC)
- Key functionality includes:
  - normalization of disparate data formats
  - ability to query (indexed) normalized data
  - visualization
  - rule-based alerting
  - reporting

Example SIEM Alerts/Queries

After-Hours Print Jobs

- Collect information on all print jobs that take place outside of normal business hours
  - "Normal business hours" can vary between departments or individuals

Large Emails to External Recipients

- Collect information on all emails that exceed specified threshold size that were sent to a recipient outside of the organization
  - Covers large attachments and large text bodies

Specific Alerts from Data Loss Prevention Systems

- Alert on "very high" severity events
  - Specific event types (USB insertion)
  - File movement from specific file shares or folders

SIEM Tools

OSSIM (https://www.alienvault.com/products/ossim/compare)

- Provides asset discovery and inventory, vulnerability assessment, IDS and behavioral monitoring

Logalyze (http://www.logalyze.com/)

- Focuses mainly on log aggregation

Enterprise Log Search and Archive (https://github.com/mcholste/elsa)

- Focuses mainly on log aggregation and indexing

The Elastic Stack a.k.a. The ELK Stack (https://www.elastic.co/)

- Scalable, distributed architecture

Analytics

Analytics

- Analytics tools extend the query and alerting functionality of the SIEM. They can implement advanced machine-learning and statistical techniques to uncover and alert on anomalous activity.
- Key functionality includes:
  - Rule-based detection
  - anomaly detection
  - risk scoring/prioritization
  - predictive analytics
  - text mining and analytics
  - Additional visualization
  - analysis interface
- Data Scientists

Analysis Tools

Programming Language of Choice

Weka

- http://www.cs.waikato.ac.nz/ml/weka/

RapidMiner

- https://rapidminer.com/

Apache Solr

- https://lucene.apache.org/solr/

Machine Learning

- Theano https://github.com/Theano/
- TensorFlow https://www.tensorflow.org/

Digital Forensics

Digital Forensics and Investigations

- Digital forensic tools to support investigations and allow a properly trained individual to preserve, collect, and analyze digital artifacts on a system or device.
- Key functionality includes:
  - digital evidence acquisition
  - artifact extraction and analysis

Digital Forensics and Investigations - Statistics

Responding to malicious insider threats requires the ability to perform digital forensics to preserve evidence of crime.

- According to the 2014 US State of Cybercrime Survey* companies did not refer legal action
  - Lack of evidence/not enough information to prosecute (36%)
  - Couldn't identify individual(s) responsible (37%)
  - Concerns about liability (8%)
- Consult with legal to understand if tools, processes, policies can withstand legal scrutiny.

Digital Forensics and Investigations Tools

Autopsy

- https://www.sleuthkit.org

Volatility

- http://www.volatilityfoundation.org/

SANS Investigative Forensic Toolkit (SIFT)

- https://digital-forensics.sans.org/community/downloads

CERT Forensics Tools https://forensics.cert.org/

- AfterLife
- DINO -Drop In Network Observer https://forensics.cert.org/dino/
- LATK https://forensics.cert.org/latk/

Notes on Tools - 1

Implementation Costs

- Hardware
- Software
- Personnel

Risk Analysis & Cost Benefit

- Commercial vs. Open Source
- True costs, support, expertise

Testing

- Always test solutions on a non-production system.
- Verify it meets need and will work in your environment.

Legal Issues

- Consulting legal counsel before deploying certain technologies
  - Protect privacy and legal rights of employees
  - Examples: content filtering, email monitoring, activity monitoring
- Review Licensing Agreements

Notes on Tools - 2

Who are the developers?

- What type of support is available?
- Have the developers been actively working on the product?

What Privileges are required for it to function?

- Administrator?
- Why are these permissions needed?

What communication channels are observed?

- What are the ports and protocols in use?
- Does this present a risk?

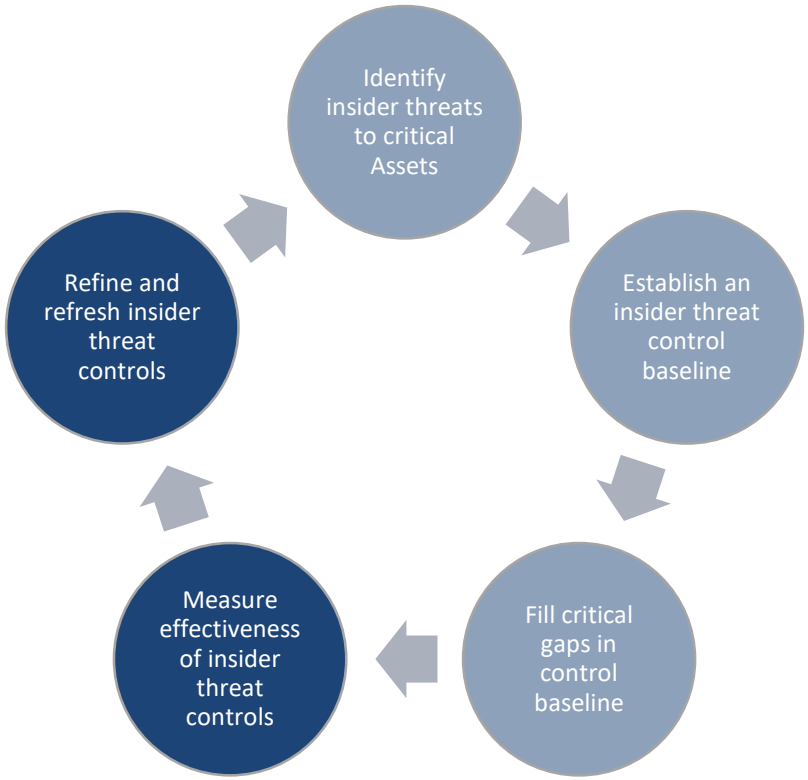
What types of data are flowing in and out of a given enclave?

- Is the product attempting to contact a cloud server? – Why?
- Can you explain why data is flowing between enclaves?

Does the software present additional risks?

- Data Exfiltration
- Sabotage

Implementing and Operating Tools



Measuring Effectiveness

Coverage

- % of endpoints monitored

True/False Positive/Negatives for Detective Controls

- Important to understand the difference between a faulty detective control (cameras record black and white video) and a bad insider threat indicator (insiders wear blue shirts)

Impact

- Reduced latencies in processes (IR, investigations, etc.)
- # of malicious actions prevented / recovered before harm done

Testing Effectiveness

Tabletops

- Exercise stakeholder's abilities to execute on policies / procedures and identify any critical gaps

Penetration Testing

- Exercise controls' abilities to prevent / detect / respond to technically sophisticated attacks

Advanced Techniques

- Wallnau et. al – insert synthetic threat data into operational data sets, measure detective controls' abilities to differentiate threat data from benign activity
- Greitzer et. al – measure predictive models against known incident data

Insider Threats are Dynamic . . .

The threat landscape changes

- Disruptive technologies
- Organization-level events
  - Mergers, acquisitions, reductions in force, etc.
- Current events
- The workforce changes

Your organization's appetite for risk changes

Stuff breaks

- "Why isn't that data in the SIEM anymore?"

. . . So Your Controls Must Also Be Dynamic

Implement periodic:

- Re-assessments of the highest priority insider threats to your organization's critical assets
- Tests designed to measure the effectiveness of the deployed insider threat controls
- Improvements to deployed controls based on testing and feedback from insider threat program stakeholders

Wrap Up

Summary

- Five categories are starting points but not exhaustive
- Determine pre-existing controls and what features you can already address
- Focus on obtaining and implementing controls at the feature level
  - Understand that tools and categories have overlapping functionality
- Begin with using the free or low cost tools during the early stages of an insider threat program for smaller networks or organizations

Contact Information

Derrick Spooner
Insider Threat Technical Solutions Team
CERT National Insider Threat Center (NITC)
Email: dspooner@cert.org

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