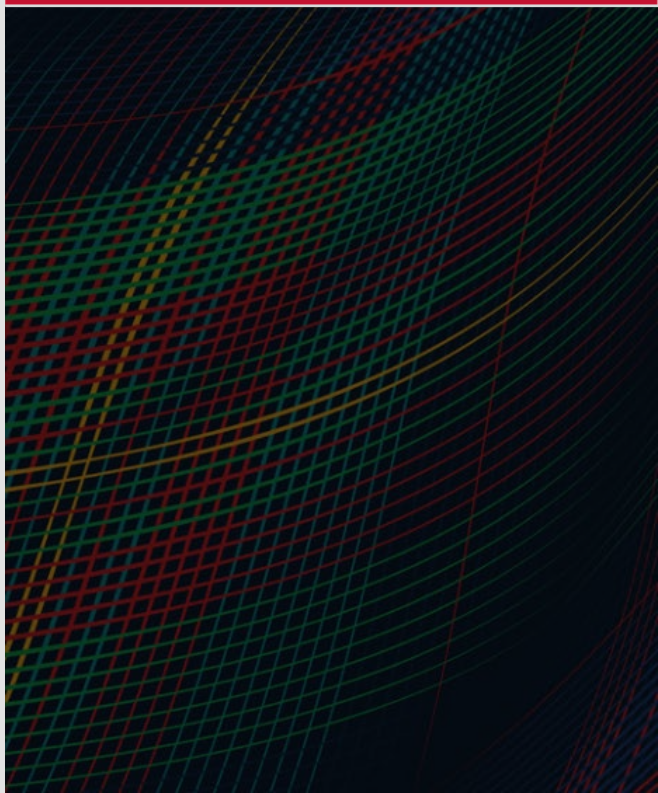
Carnegie Mellon University
Software Engineering Institute

Designing and Implementing a Cyber Insider Threat Mitigation Program

SEPTEMBER 4, 2024

Randall (Randy) Trzeciak
Deputy Director; Cyber Risk and Resilience
CERT Division; Software Engineering Institute



Document Markings

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

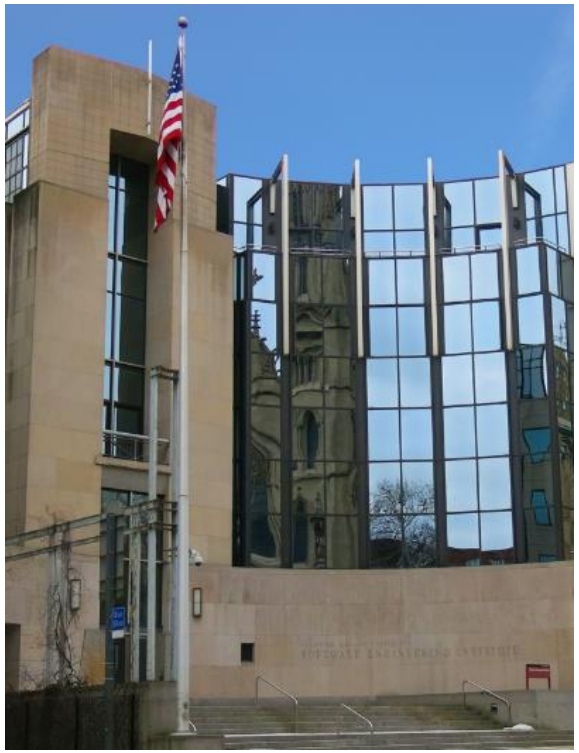
This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® and Carnegie Mellon® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM24-0046

CMU Software Engineering Institute (SEI)

Carnegie Mellon University Software Engineering Institute



Bringing innovation to the U.S. government

- A Federally Funded Research and Development Center (FFRDC) chartered in 1984 and sponsored by the DoD
- Leader in researching complex software engineering, cyber security, and artificial intelligence (AI) engineering solutions
- Critical to the U.S. government's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

CERT Division – Insider Threat Focus Area

Carnegie Mellon University Software Engineering Institute

Center of insider threat expertise

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

Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber and physical threats

Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats

Building an Insider Risk (Threat) Program

Carnegie Mellon University
Software Engineering Institute

The Need for an Insider Risk Program

Carnegie Mellon University Software Engineering Institute

In the past year(s), organizations have seen several serious data breaches committed at the hands of insiders.

As tactics and techniques improve in sophistication, organizations must have dynamic processes to help them “stay on top” of the latest threats and vulnerabilities.

Motivation for a Program

Carnegie Mellon University Software Engineering Institute

"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

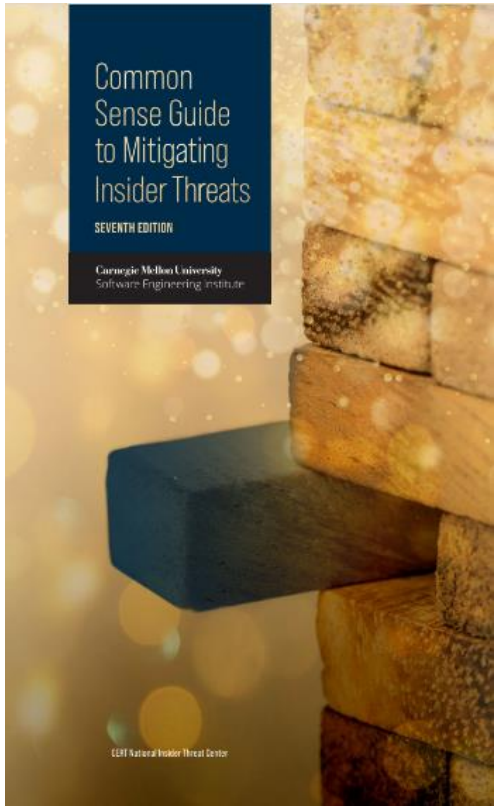
To be prepared and ready to handle such events in a consistent, timely, and quality manner including understanding

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

What is an Insider Risk Program?

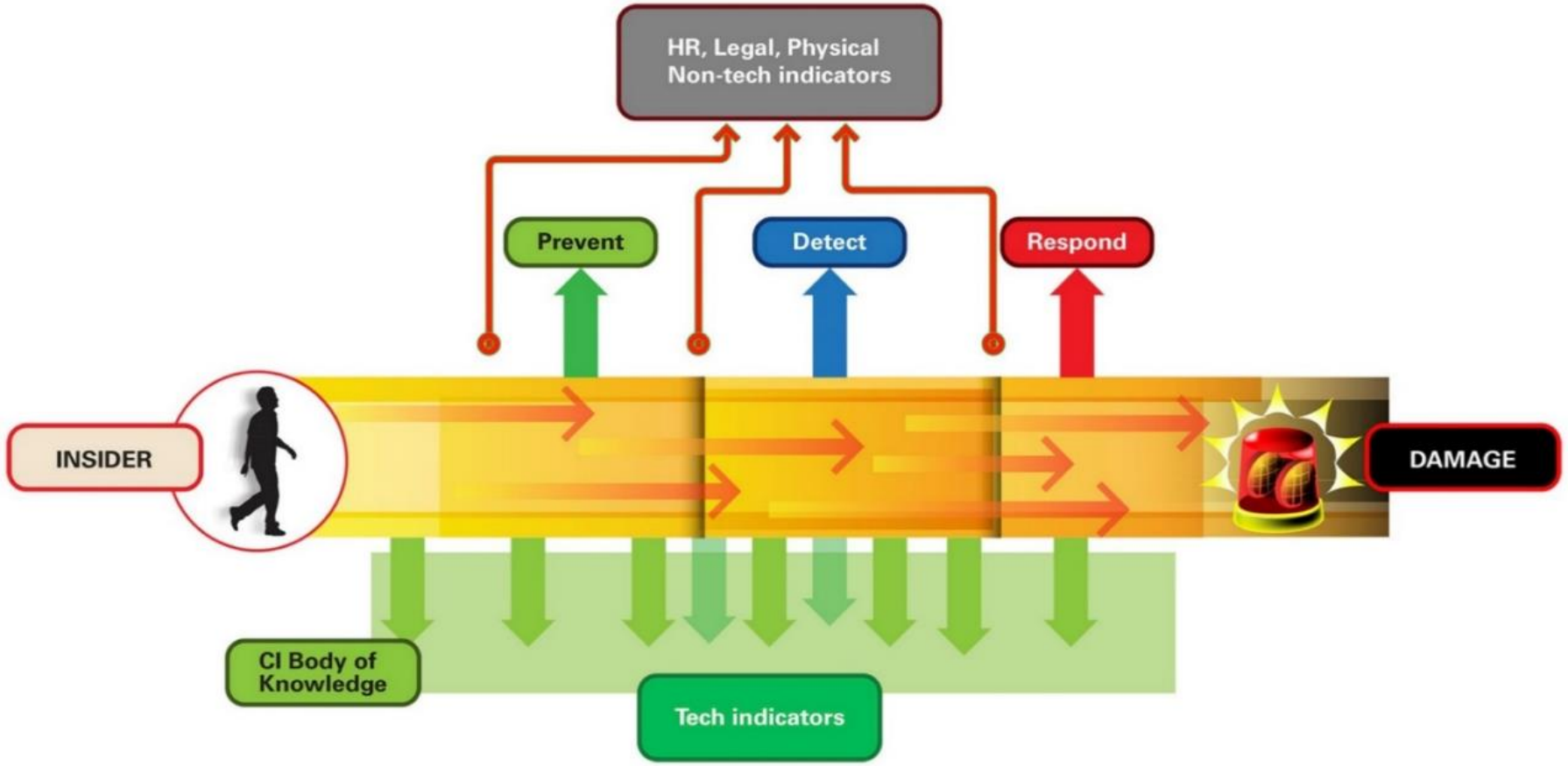
The CERT *Common Sense Guide to Mitigating Insider Threats 7th Edition* defines an insider threat program (InTP) as an enterprise-wide program with

- an established vision
- defined roles and responsibilities for those involved
- specialized awareness and training for all involved
- criteria and thresholds for
  - data collection and analysis
  - declaring insider threat activity and risks
  - conducting inquiries
  - referring to investigators
  - requesting prosecution
- supporting policies, procedures, and practices
- a process to ensure privacy and confidentiality
- management's support



https://resources.sei.cmu.edu/asset_files/WhitePaper/2022_019_001_886876.pdf

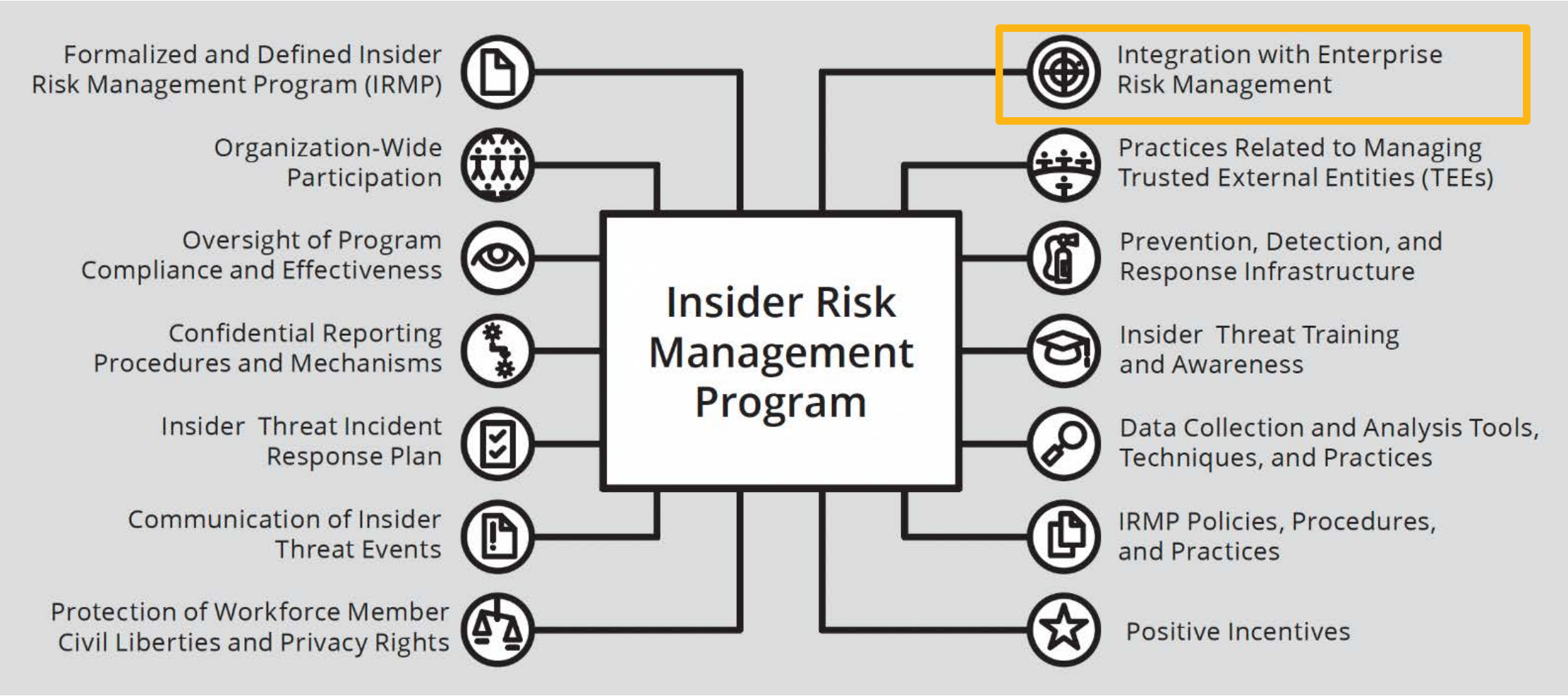
The Goal for an Insider Threat Program…



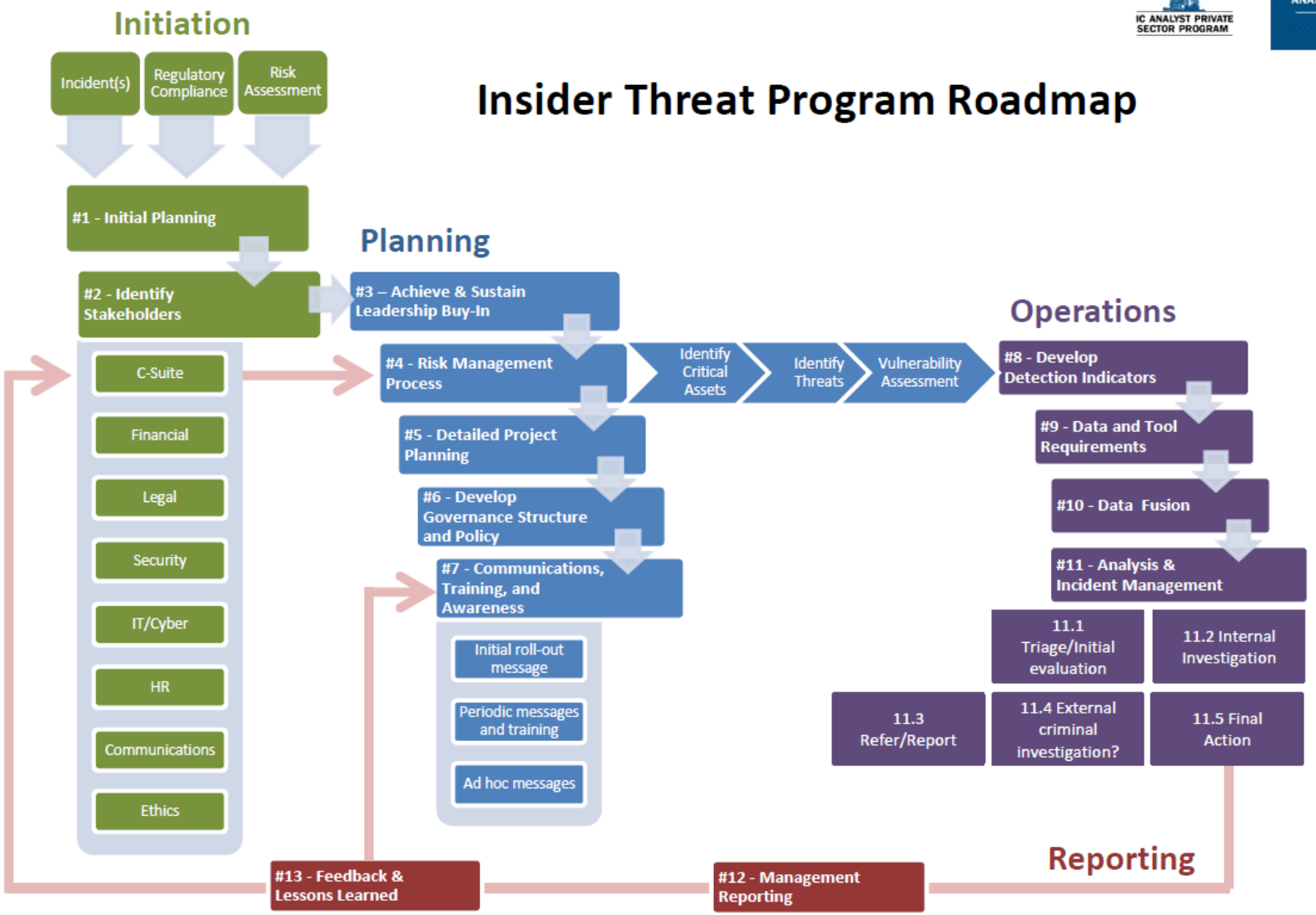
Is to reduce insider risks to critical assets to acceptable levels

https://insights.sei.cmu.edu/insider-threat/2020/01/maturing-your-insider-threat-program-into-an-insider-risk-management-program.html

CERT Insider Threat Program Key Components – It Starts With Risk Management



Building an Insider Threat Program



Source: https://www.insaonline.org/insider-threat-roadmap/

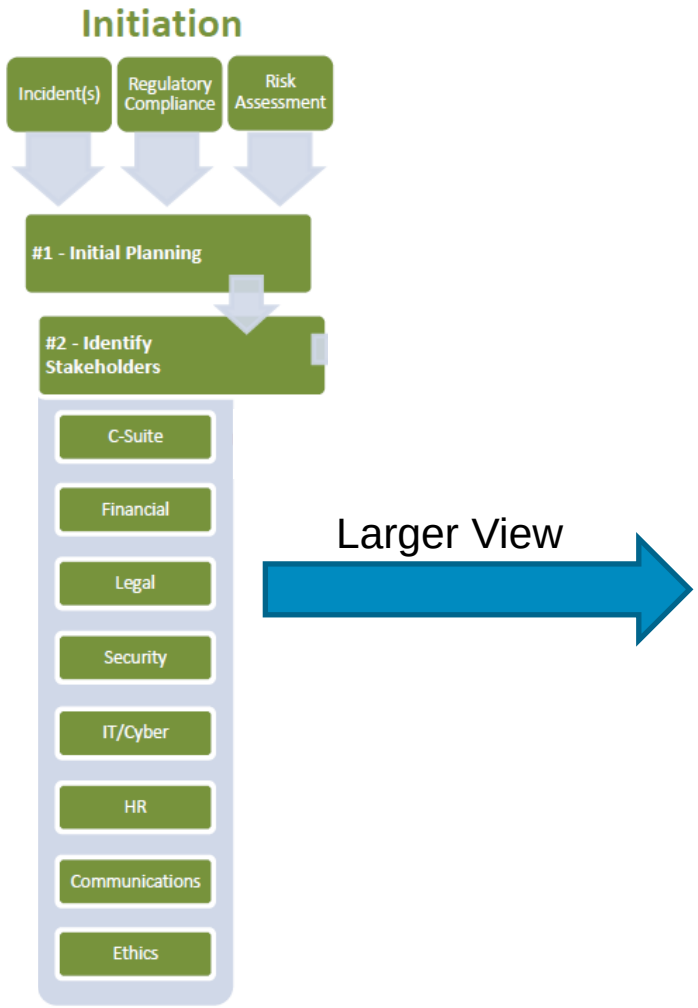
Step #1 – Initial Planning

Building a Business Case for an Insider Threat Program

- Use a risk management thought process
- Include:
  - the problem you are trying to solve
  - the scope and impact of the program
  - the approach to solving the problem (and why it is better than alternatives)
  - the possible positive outcomes of the program
  - the possible risks associated with the program
  - the possible risks associated with *NOT* doing the program

Source: https://www.insaonline.org/insider-threat-roadmap/

Step #2 – Stakeholder Planning



Larger View

- C-Suite
- Financial
- Legal
- Security
- IT/Cyber
- HR
- Communications
- Ethics

Source: https://www.insaonline.org/insider-threat-roadmap/

Step #2 – Stakeholder Planning

Additional Potential Stakeholders

- Enterprise Risk Management
- Privacy/Civil Liberties Office
- Employee Relations/Ombudsmen
- Unions/Collective Bargaining Units
- Top Line Business Unit Leaders
- Behavioral Sciences (BS)
- Counterintelligence (CI)
- Data Owners

Source: https://www.insaonline.org/insider-threat-roadmap/

Keys for Successful Stakeholder Identification and Engagement

Carnegie Mellon University Software Engineering Institute

Keys to success include:

- Identifying stakeholders as early as possible
- Continually evaluating the list for needed additions
- Creating a communication strategy that is inclusive and bi-directional
- Meeting frequently, both as a group and in individual settings (where appropriate)

Establish Relationships and Engagement

Carnegie Mellon University Software Engineering Institute

Support and engagement can include:

- senior leader assigned as director/head of the insider threat program (*different than the InTP manager*)
- memos to key stakeholders, business process owners, and organizational senior management
- strategic meetings with key stakeholders
- stakeholder attendance at planning meetings
- ongoing references to insider threat issues in meetings, publications, and training

Key Requirements for Program Success

Carnegie Mellon University Software Engineering Institute

To achieve success requires:

- commitment and sponsorship from all levels of management
- acceptance and buy-in across the enterprise
- recognizing what's already in place in your enterprise
- a long-term vision for the program
- a persistent planning & implementation/working group
- a project plan to track goals and milestones
- iterative short-term tasking and pilot activities

Common Documents to Build an Insider Threat Program

There are a core set of documents that most organizations need in order to formalize the Insider Threat Program:

- Insider Threat Policy (*you will*)
- Insider Threat Charter (*you will what*)
- Concept of Operations (CONOPS) (*you will how*)
- Implementation Plan (*how you will get there*)
- Incident Response Plan (*what to do when something happens there*)
- Communications Plan (*who/how to tell what happened there*)

Run Everything Through Legal/Privacy

Carnegie Mellon University Software Engineering Institute

Before creating these documents:

- Work with legal counsel and privacy officers in the development of the Insider Threat Program
- Make sure both groups have ongoing involvement with process/procedures involving investigations and dispositions of inquiries.
- Ensure that all Insider Threat Program actions meet legal mandates and protect the rights and privacy of employees.

Insider Threat Program Team Experience/Skills

Carnegie Mellon University Software Engineering Institute

We have seen organizations hire people with the following skills:

- Investigative experience
- Law enforcement experience
- Counterintelligence or intelligence experience
- Senior systems analysis experience
- Program management experience
- IT security and defense in depth experience
- Digital investigation or analysis experience
- Statistical analysis experience
- Insider threat technology experience

Insider Threat Data Analytic Hub

Carnegie Mellon University
Software Engineering Institute

Insider Threat Hub

Insider Threat Hub: A centralized capability for insider threat data collection, correlation, analysis and response

Common hub capabilities

Collect, correlate, and aggregate data from disparate sources.

Develop, deploy, and refine indicators of potential insider activity.

Evaluate detected instances of potential insider activity.

Provide supporting information to incident investigators and responders.

An insider threat hub is NOT a specific tool, but typically a collection of tools and capabilities.

Benefits of an Insider Threat Hub

Allows the insider threat team to discreetly identify anomalies and analyze potential insider threat activity

Produces a better “whole person” picture and provides contextual information to potential insider threat activity

Can facilitate information sharing across previously stove-piped groups within an organization

Staffing the Hub

Analysts

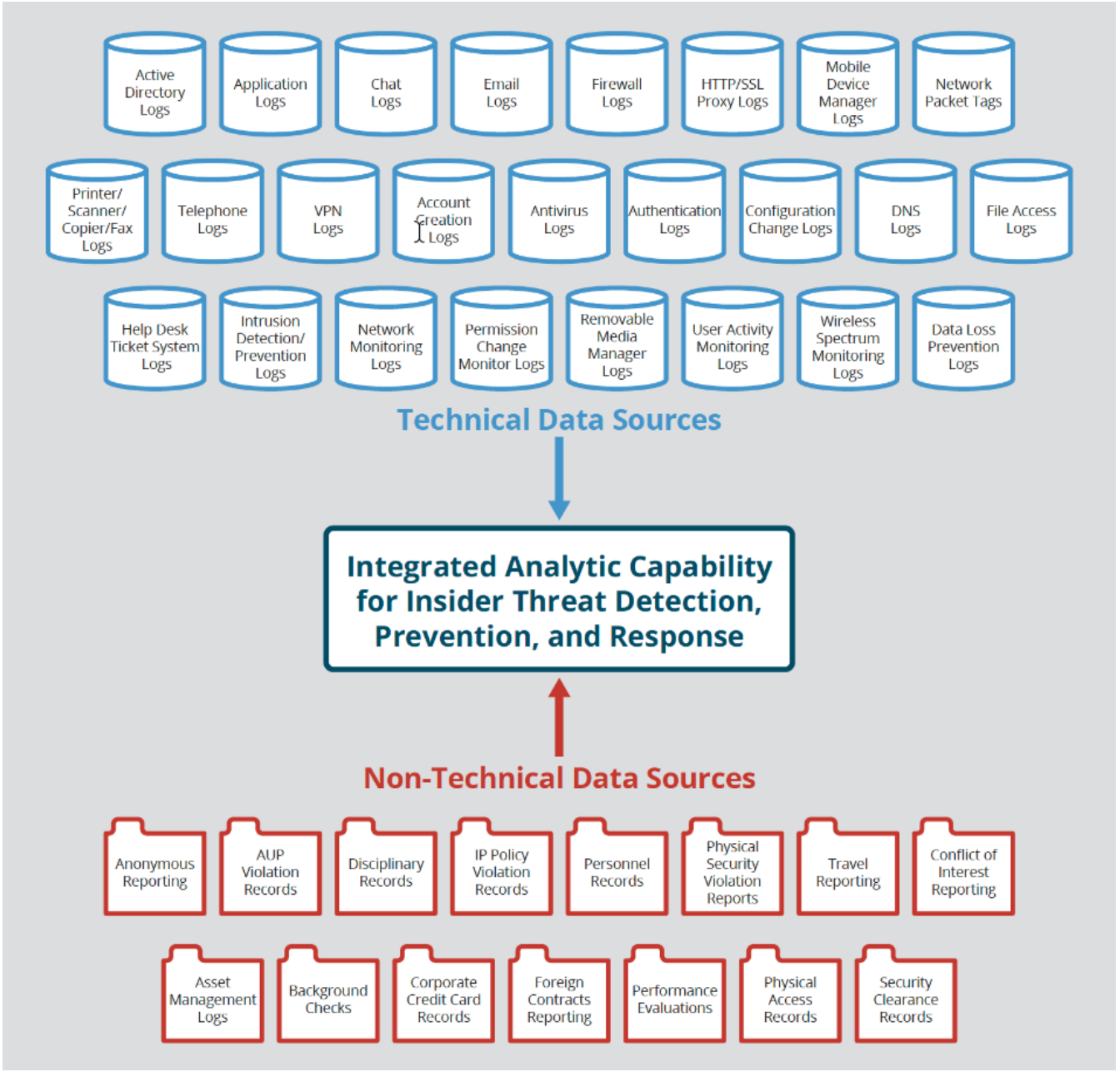
- **IT skills** – understand the data sources
- **CI/investigative skills** – build the story
- **Behavioral science** – understand motives and patterns
- The number of analysts needed depends on a number of factors, including InTP scope and degree of security automation present

Support

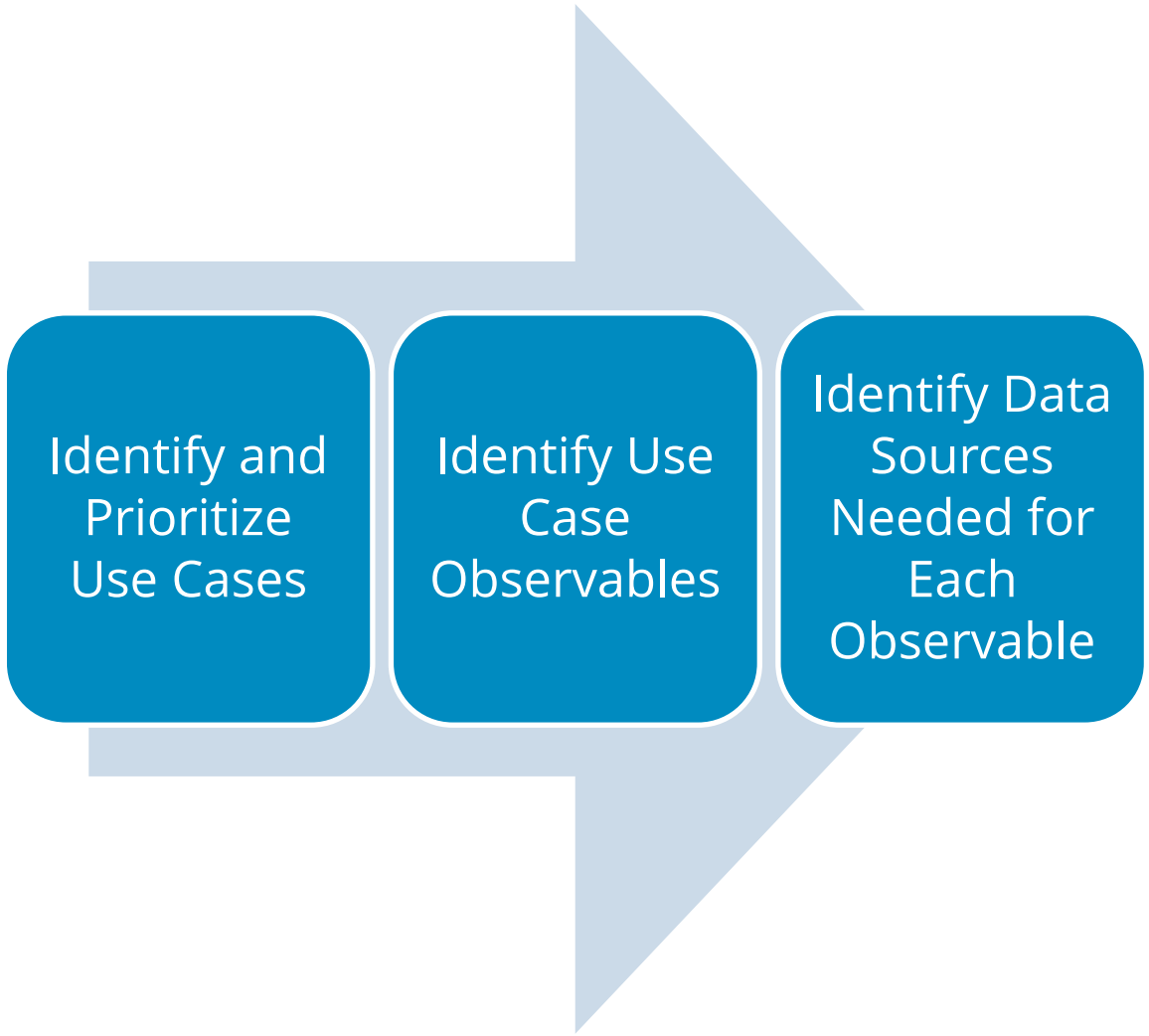
- **Machine Learning, Data Science** – configure the systems that process massive amounts of data
- **Behavioral Scientists** – develop potential behavioral indicators
- **IT Support** – build and support these systems

Management

- **Program Manager** – coordinates hub operations, acts as liaison to the rest of the InTP



Data Source Selection



A use case-based approach is the key to success.

- Enables effective prioritization of limited resources
- Facilitates development of clear data access request justifications
- Aligns with risk management processes
- Promotes effective participation of InTP stakeholders

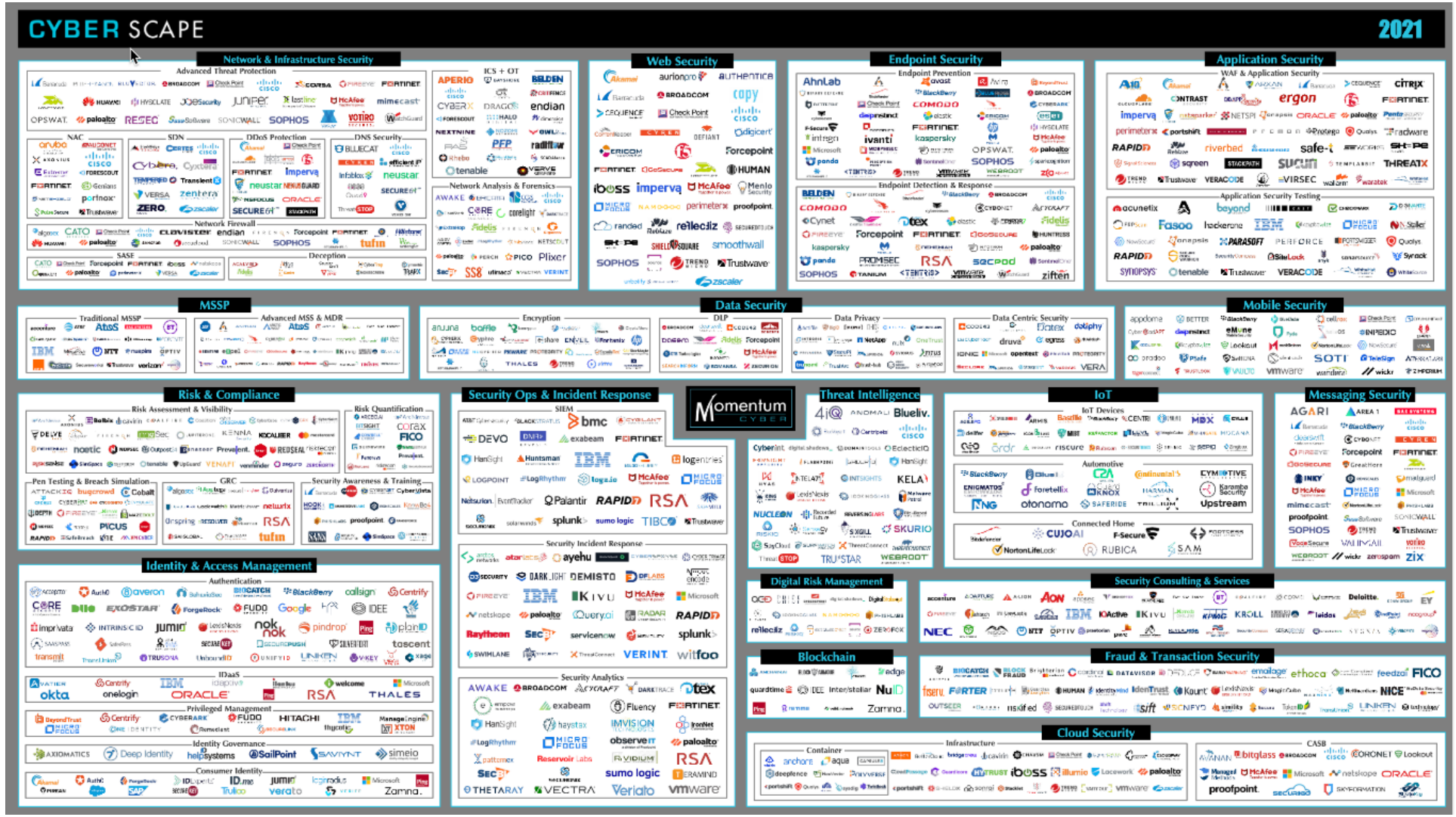
Hub Analysis Strategy

Carnegie Mellon University Software Engineering Institute

Create a high-level view of information that can prioritize alerts and observables based on severity.

Prioritize analysis according to the following:

The Tool Landscape Is Vast



https://momentumcyber.com/docs/Yearly/2022_Cybersecurity_Almanac_Public_Edition.pdf

Purpose of Tools

Tools provide two main purposes

- Main Insider Threat Hub tools
  - Data Loss Prevention (DLP)
  - Security Incident and Event Management (SIEM)
  - User Activity Monitoring (UAM)
  - User/Entity Behavioral Analytics (UEBA)
  - Knowledge Management
- Supporting tools
  - Digital Forensics
  - Analytics
  - Identity Management (IAM/PAM)

Avoiding Vendor Lock-In

Ask yourself: where are the requirements and designs for your detective controls being documented?

- If the answer is ‘in my UAM/SIEM/UBA tool’, then changing tools will be a significant challenge

Consider a repository for controls where you document things like

- Detailed descriptions for the control
- Associated threat scenarios and / or indicators
- Revision history to the control
- Measures of effectiveness

Unintended Consequences of an Insider Threat Program

Carnegie Mellon University
Software Engineering Institute

Perception of the Insider Threat Program -1

Carnegie Mellon University Software Engineering Institute

Negative media terminology

- Snitch
- Tattletale
- Ratting on fellow employees
- Big Brother
- Report suspicious actions of their colleagues
- Impact to legitimate whistleblowing
- Internal Affairs

Perception of the Insider Threat Program -2

Carnegie Mellon University Software Engineering Institute

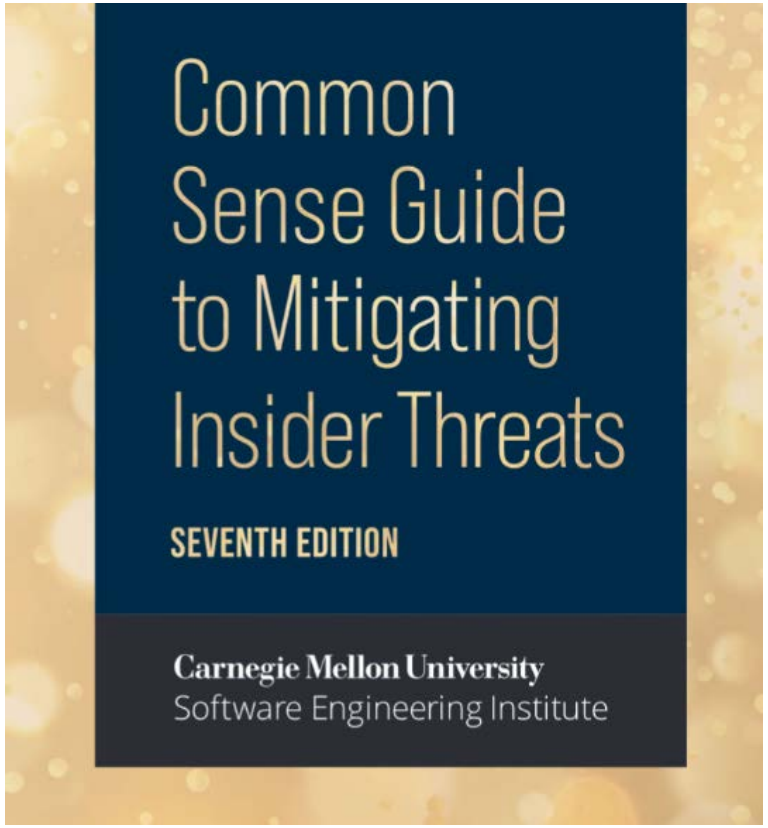
Alternate Naming Considerations

- Asset protection program
- Corporate Compliance Monitoring
- Enterprise Protection Program
- Employee Protection Program
- Enterprise Threat Management Program
- Internal Risk Management Program

Resources

Carnegie Mellon University
Software Engineering Institute

Common Sense Guide to Mitigating Insider Threats, 7th Edition



- Best practices for preventing, detecting, and responding to insider threats and managing insider risk
- What's New?
  - 22nd Best Practice: Learn From Past Insider Incidents
  - Updated standards crosswalk
  - Updated best practice on insider risk management program building
  - Updated case studies and statistics from the CERT Insider Incident Repository
- https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=886874

Common Sense Guide to Mitigating Insider Threats

1 - Know and protect your critical assets.	12 - Deploy solutions for monitoring workforce member actions and correlating information from multiple data sources.
2 - Develop a formalized insider risk management program.	13 - Monitor and control remote access from all endpoints, including mobile devices.
3 - Clearly document and consistently enforce administrative controls.	14 - Establish a baseline of normal behavior for both networks and workforce members.
4 - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	15 - Enforce separation of duties and least privilege.
5 - Anticipate and manage negative issues in the work environment.	16 - Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
6 - Consider threats from insiders and trusted external entities in enterprise-wide risk assessments.	17 - Institutionalize system change controls.
7 - Be especially vigilant regarding social media.	18 - Implement secure backup and recovery processes.
8 - Structure management and tasks to minimize unintentional insider stress and mistakes.	19 – Mitigate unauthorized data exfiltration.
9 - Incorporate insider threat awareness into periodic security training for all workforce members.	20 - Develop a comprehensive workforce member termination procedure.
10 - Implement strict password and account management policies and practices.	21 - Adopt positive incentives to align the workforce with the organization.
11 - Institute stringent access controls and monitoring policies on privileged users.	22 – Learn from past insider threat incidents.

Point of Contact

National Insider Threat Center
Randall F. Trzeciak
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
rft@cert.org – Email

http://www.cert.org/insider_threat/