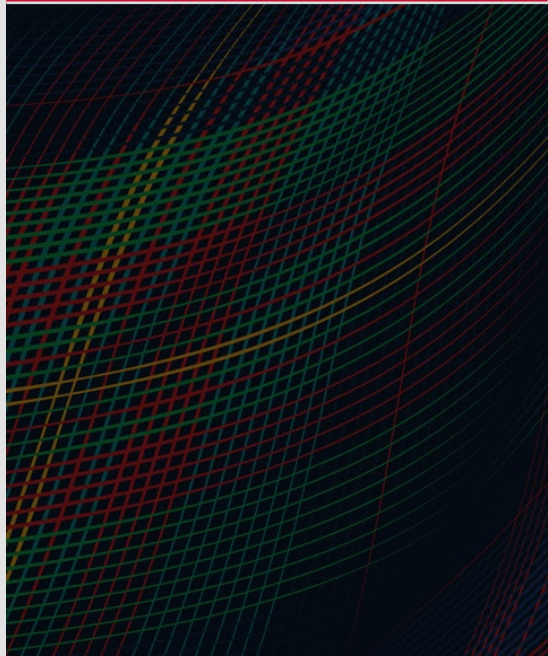
Measuring the Effectiveness of a Cyber Insider Threat Mitigation Programme

SEPTEMBER 5, 2024

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

Carnegie Mellon University
Software Engineering Institute



Document Markings

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

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

Insider Threat Program (InTP) Building Success Criteria – Where to Start

Carnegie Mellon University
Software Engineering Institute

Insider Threat Program (InTP): Knowing What's in Place

Component	Not Implemented	Partially Implemented	Fully Implemented	Not Applicable
Awareness of Insider Threat as a Problem		X		
Executive Management Support			X	
Organizational Participation	X			
Policies and Procedures	X			
Insider Threat Controls and Defenses		X		
Technical Data Sources Collected			X	
Behavioral Data Sources Collected	X			

Insider Threat Program (InTP) Effectiveness Measures

Carnegie Mellon University
Software Engineering Institute

Why Metrics Matter

Security and security initiatives at large are seen as cost centers (i.e., security doesn't make the enterprise money), so justification of expenditures is critical.

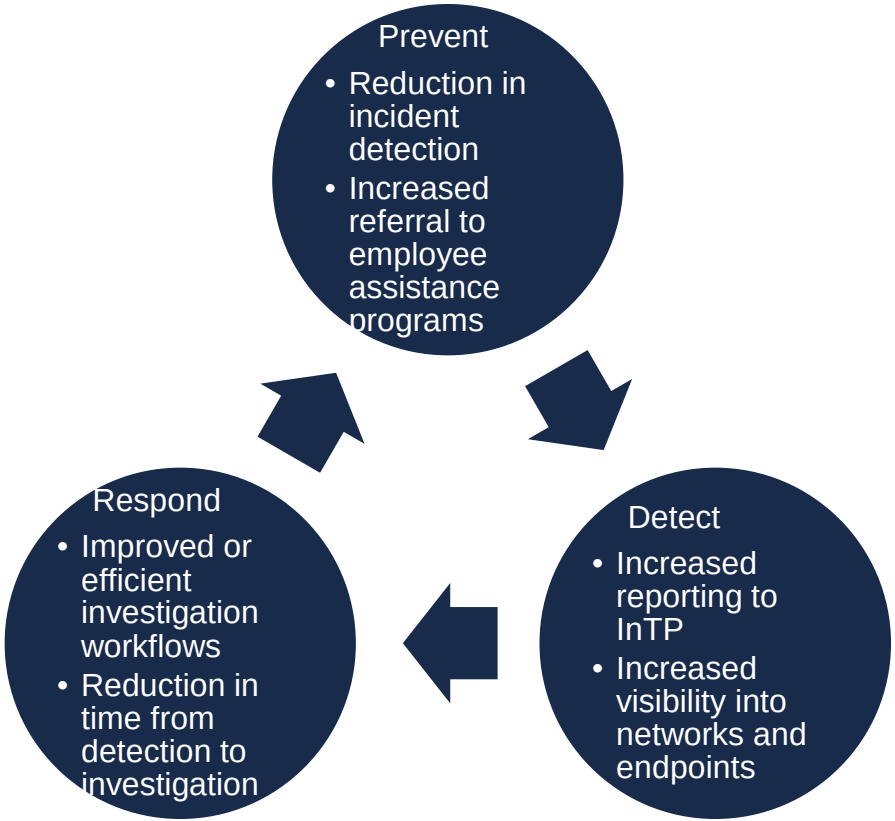
If you can't communicate out the value of your Insider Threat Program to stakeholders and decision makers, then the InTP's work will not be as impactful.

- The InTP's activities and impact should make sense not just to the team, but to those outside of the team.

Measurement is a component of knowledge management and enables program improvement.

- Documentation of metrics and improvement activities may be relevant to regulators or other external stakeholders.
- You cannot make informed decisions without data.

Different Metrics for Different InTP Functions



Different Metrics for Different Audiences

Quantitative vs Qualitative Metrics

Carnegie Mellon University Software Engineering Institute

Quantitative

- *Counting* or numbers-based metrics, such as
  - "number of _"
  - "percentage of _"
- Examples:
  - Referrals and reports from staff
  - Investigations
  - Incidents detected
  - Incidents referred to law enforcement
  - Sites blocked
  - Assets recovered
  - Loss prevented

Qualitative

- Descriptive metrics, such as
  - how well something is performed
  - how well something is managed
  - quality measures
- Examples:
  - Security culture
  - Training and awareness leading to increased reporting
  - Identification of broken processes
  - Case study
  - Incident severity / criticality
  - Improvement of or contribution to reporting requirements from InTP

Sample Quantitative Metrics with Examples

These IT and investigation-focused metrics may be easier to calculate during program infancy, but also track against previous measures over time.

Coverage

- Percentage of systems covered by a host-based user activity monitoring system

Latency

- Average time between malicious activity and discovery by Insider Threat team

Compliance

- Percentage of recommended/required controls implemented

Impact

- Number of incidents prevented, reduction in time to resolve investigations, reduction in number of incidents over time

Enterprise-wide vs Program-specific Metrics

Enterprise-wide

Changes in individual business units before and after the instantiation of the InTP

Examples:

- Implementation and management of necessary controls
  - e.g., pre-employment screening, code of conduct, DLP, mandatory vacation policies, and investigation teams

Program-specific

What InTP team members accomplish

Examples:

- Insider event/incident counts
  - e.g., leads, inquiries, investigations, cases closed
- Reports of incidents escalated incidents to management and law enforcement referrals.

Success vs Value Metrics

Success

May be more quantitative, more narrow or tactical view of InTP operations

Examples:

- Behavioral conduct risks determined
- Process reviews
- Policy Violation warning letters sent
- Cases referred to law enforcement or external partners
- Departing employee / Offboarding reviews of accounts
- Extent to which the InTP has or is accomplishing its objectives

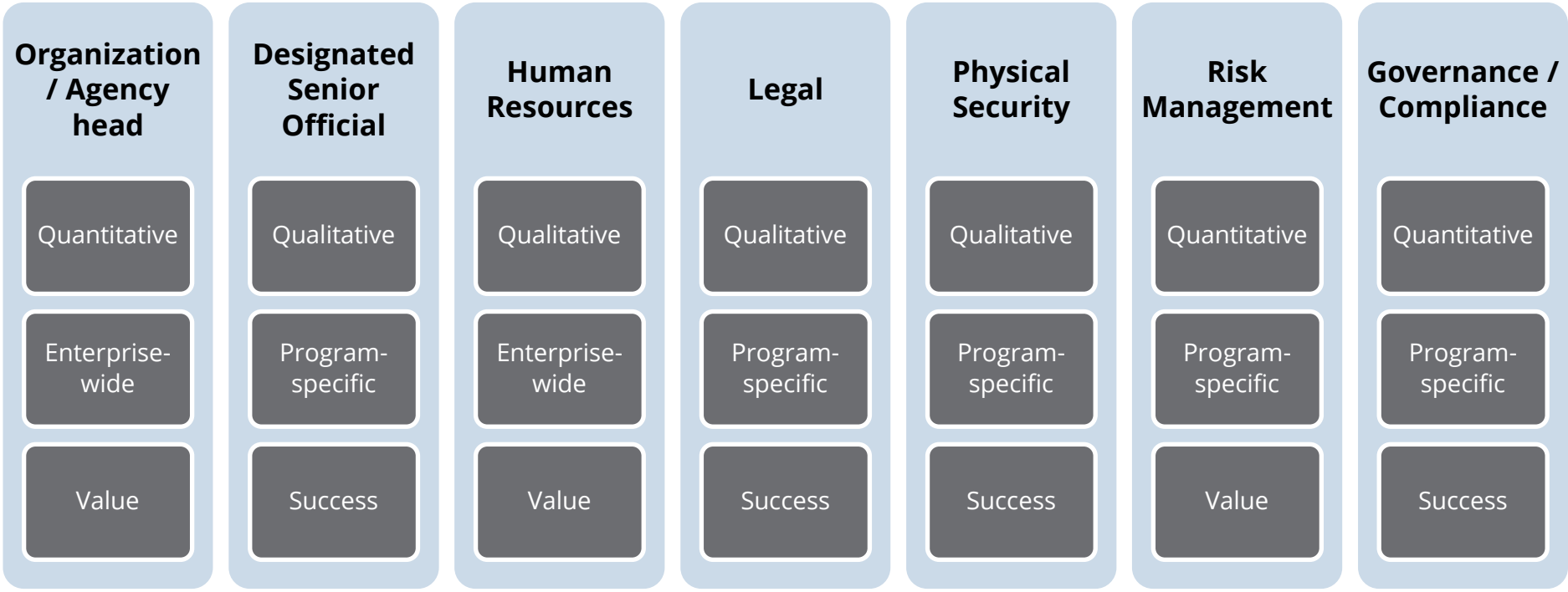
Value

How the program is able to enable the business lines to do what they do better, or how the enterprise is better for having an InTP

Examples:

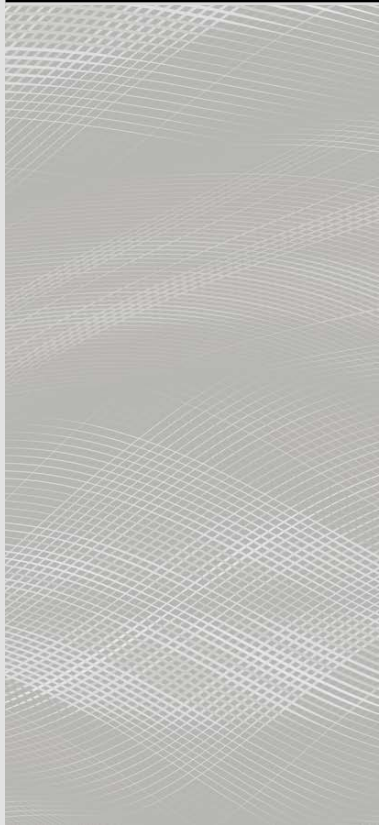
- Risk avoidance where the Insider Threat program is able to proactively identify any issues where the risk can be mitigated.
- Implementation of policy changes and improved work behaviors that followed.
  - e.g., significant drop in non-work related internet activity when monitored staff were required to sign a User Activity Monitoring Acknowledgement

Potential Metrics of Interest



Return on Investment (ROI): The Big Question

Carnegie Mellon University
Software Engineering Institute



ROI for an InTP Challenges

Carnegie Mellon University Software Engineering Institute

Before the program is built

- Some organizations want an ROI estimate before starting a program
- Calculations have to be made almost entirely on conjecture

Program start

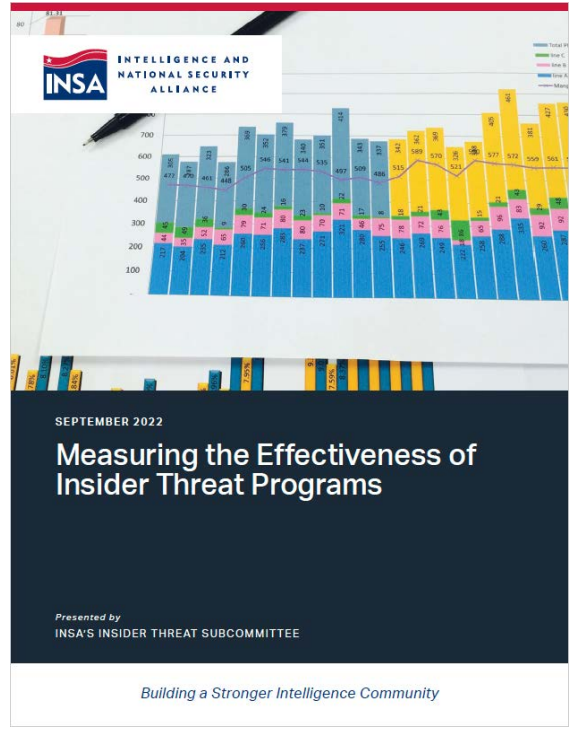
- Upfront costs for tools and starting a program may make it appear the costs outweigh any potential benefit
- Calculating ROI for every purchase or hire becomes unwieldy

Ongoing ROI calculations

- Insider threat is not a revenue-generating function
  - Not unique to InTP, often applies to Security in general
- To calculate ROI for InTP, potential inputs for Revenue and Cost must be identified.

ROI and Measures of Effectiveness

- Establishing appropriate metrics supports justifications for resources (budget and personnel) and sustains support from senior leader and stakeholders
- In an informal INSA survey, to learn if InTP practitioners can measure their programs' effectiveness, only 32% said they could determine the effectiveness of their program
- Indicating organizations need to understand the importance of MoE and ROI for their programs
  - InTP managers need to learn how to develop such metrics



https://www.insaonline.org/docs/default-source/default-document-library/2022-white-papers/insa_wp_effectiveness.pdf

Potential Inputs for ROI

$$ROI = \frac{Profit}{Cost}$$

Carnegie Mellon University Software Engineering Institute

"Profit" *(Revenue – Cost)*

- Dollar value of any data targeted for exfiltration, or documents / IP recovered
- Incidents that result in action for each use case.
  - Multiply those counts by average data loss stats to estimate cost-saving
- Benefits of increased productivity / reduced insider threat activity

Cost

- Employee salary / wages and benefits
- Tool purchases and maintenance costs
- Hiring of consultants or investigators

Making Measurements: Assessments and Evaluations

Carnegie Mellon University
Software Engineering Institute

Example Methodologies

Methods for evaluating your InTP include but are not limited to

- assessments, including self-assessments
  - gap assessment
    - Increasing data insights where there was previously no visibility
    - Identifying gaps in administrative, physical and technical controls
  - risk assessment
  - vulnerability assessment
- testing of procedures, workflows, and skill-sets
  - tabletop exercises
  - penetration testing
  - business continuity / disaster recovery (BC/DR) tests

Mechanisms for Conducting Assessments -1

The InTP program manager, working with senior management and Legal, will need to develop mechanisms to perform any type of assessments.

Goals, objectives, and metrics for assessments will need to be developed or identified.

Mechanisms for Conducting Assessments -2

Mechanisms can include

- assessments against the National Insider Threat Task Force (NITTF) minimum standards and insider threat policy
- assessments against the organizational insider threat framework or third-party criteria
- scorecards or benchmarking against another organization or a set of standard criteria
- table top or mock incident scenario exercises
- direct testing of operations and response, including penetration testing and red/blue teaming

Testing InTP Components

You may want to test specific components of the InTP to ensure components are working properly.

Additional mechanisms for testing can include

- auditing of documented procedures against real-life actions
- interviews or surveys of participants or stakeholders to obtain feedback on how well things are operating
- piloting new components and tools

Third-Party Assessments

Various external or third-party assessments exist for both governmental and non-governmental organizations.

Department of Homeland Security (DHS): Cybersecurity and Infrastructure Security Agency (CISA) guidance for doing self-assessment:
https://www.cisa.gov/insider-risk-self-assessment-tool

Evaluating Training and Awareness

Training and awareness may require unique metrics for evaluating efficacy of any materials, but also the overall level of awareness of the workforce.

Measure	Sample Metrics	Considerations
Post-test scores	• average score • # of employees with passing scores • # of employees with passing scores on first attempt	High rates of passing on first attempt may indicate that test is too easy. Consider increasing difficulty or nuance of training content.
Pre- and post-test scores	• average change in employee scores after completing training • # of employees passing on pre-test vs post-test	Reduction in scores between the pre- and post-test suggest that training may need significant revision.
Pre-test scores and test-out	• # employees able to test-out of training sections • average amount of content that employees can test-out of • time saved on training by test-out	If employees are consistently testing out of specific components of training, then consider focusing training and awareness refreshers on these topics and re-testing.

Choosing & Reporting the Right Metrics

Carnegie Mellon University Software Engineering Institute

Think through the following questions as you develop your program's metrics.

Metrics

Team Member(s)

- Who will be reporting the metric? Do they have the experience to contextualize it?
- Which member(s) of the team have experience developing metrics?
- Does every team member have an opportunity to contribute metrics?
- What functions are under the scope of the

Audience

- What part of the organization or stakeholder will receive the information?
- Does the stakeholder have subject matter expertise?
- What are their pain points? What will they care about?
- How do they prefer to receive information?

Organizational Context

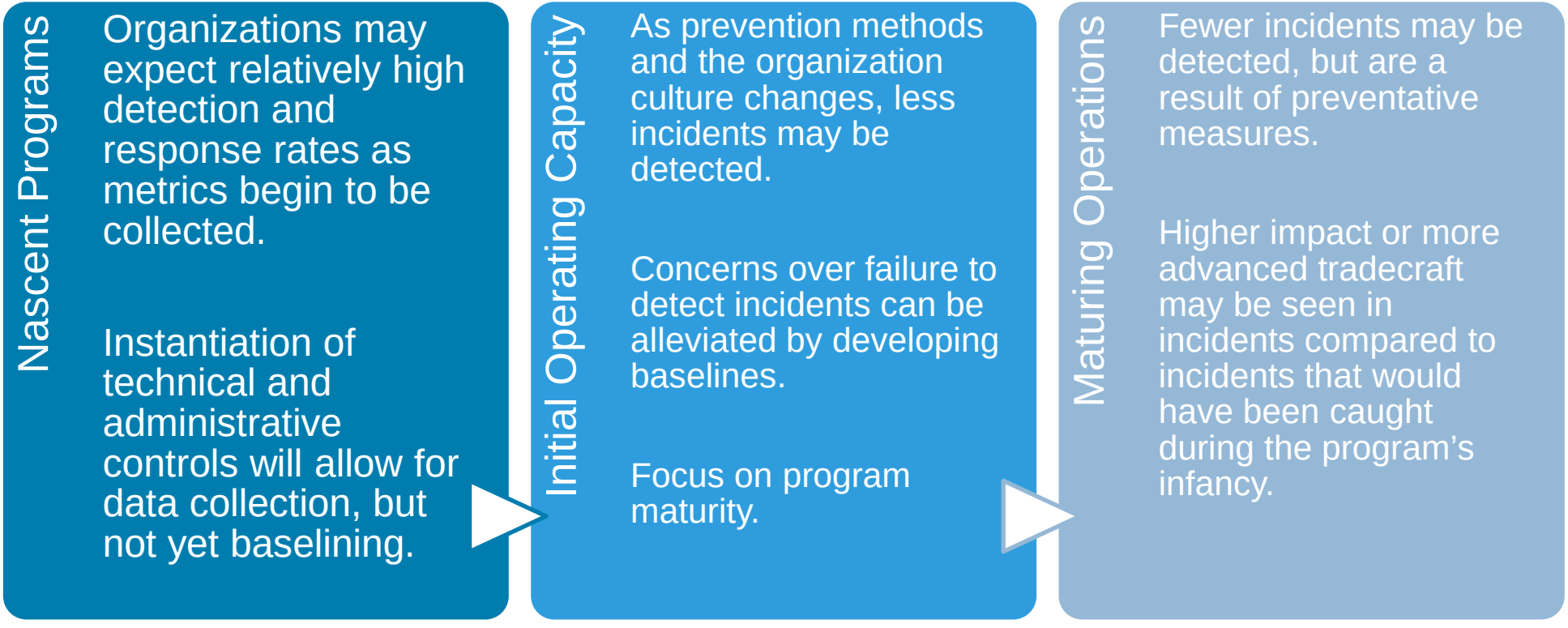
- In what manner will the metrics be reported?
- Is there an opportunity to "explain" the metric?
- Are there major changes that the organization is facing? Does this impact what you are reporting? how it is calculated?
- What are issues facing your organization's industry or sector?
- How can you benchmark events or trends?

Program Age or Maturity

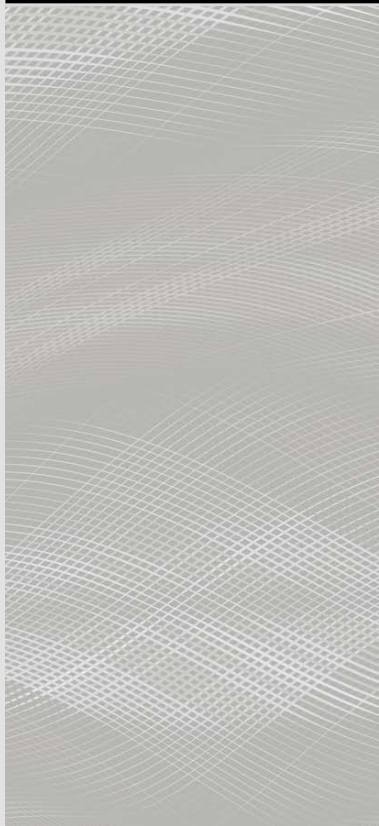
- How long have you had an insider threat program?
- Have there been any major changes to the program?
- Have there been any major changes in the organization? How has that impacted the program?
- How can you connect to the mission of the organization?

Metrics Lifecycle

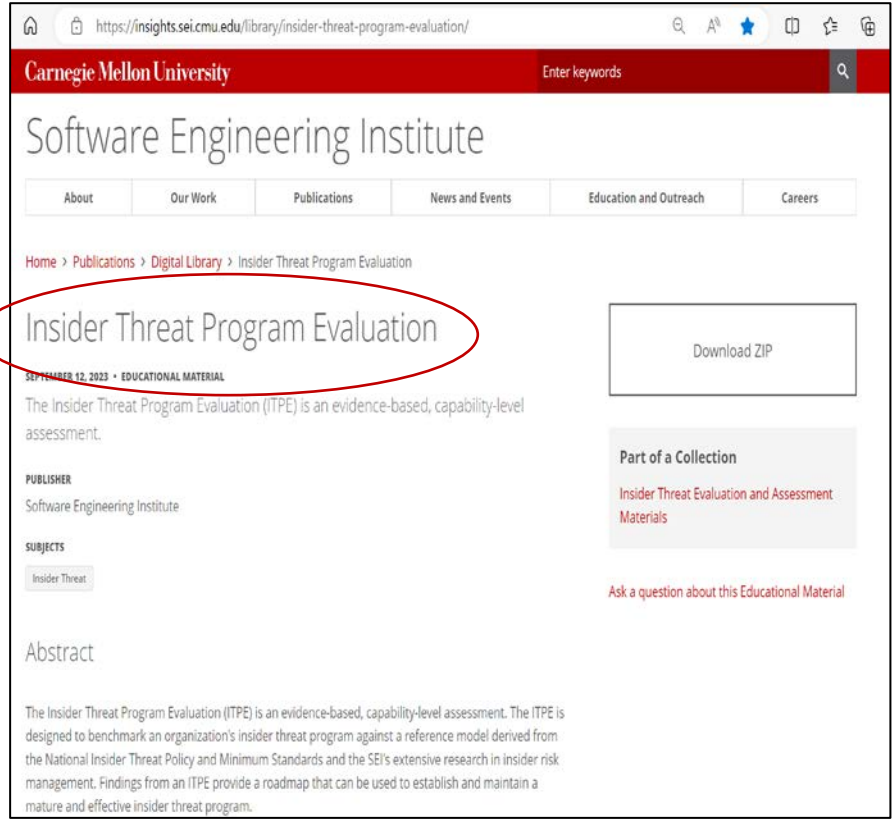
While evaluations of your Insider Threat Program within its first year(s) may be focused on gaining initial operating capacity, over time the metrics used will need to evolve.

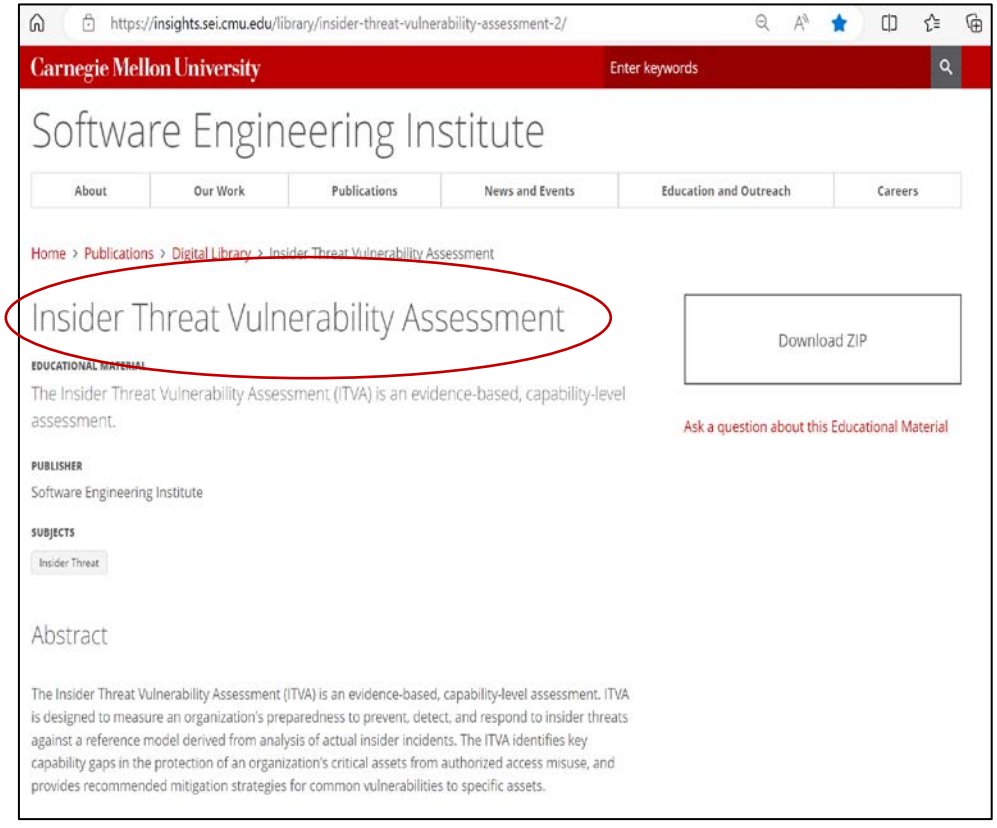


Resources



SEI / CERT Resources (Assessments) -1





Open-Source Releases for ITVA, ITPE

Available online:

- ITVA: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=983683
- ITPE: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=983664

Released materials include:

- Capability and indicator workbooks
- Process documentation
- Sample briefings for planning, execution, and reporting of assessment findings

Community feedback is welcomed and appreciated!

SEI / CERT Resources (Training) -2

Carnegie Mellon University Software Engineering Institute

Building an Insider Threat Program

RISK ASSESSMENT & INSIDER THREAT

This seven (7) hour online course provides a thorough understanding of the organizational models for an insider threat program, the necessary components to have an effective program, the key stakeholders who need to be involved in the process, and basic education on the implementation and guidance of the program. This training is based upon the...

Insider Risk Management: Measures of Effectiveness

RISK ASSESSMENT & INSIDER THREAT

This three-day, instructor-led course develops the skills and competencies needed to assess an organization's insider threat prevention, detection, and response capabilities; evaluate the effectiveness of formal insider threat and insider risk management programs; identify the maturity of an organization's insider risk management processes and...

Insider Risk Management Measures of Effectiveness (IRM-MoE) Certificate Package

RISK ASSESSMENT & INSIDER THREAT

Students who wish to purchase the certificate program package (two eLearning courses, instructor-led course, certificate exam) will receive a discount from the total cost. The program packages correspond with scheduled course dates, so select the program package that best meets your scheduling needs. The Insider Risk Management Measures of...

Education and Outreach | Software Engineering Institute (cmu.edu)

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/