Insider Threat Metrics and Measures of Effectiveness

CERT National Insider Threat Center

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. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0644

Approaches for Insider Threat Metrics

- Leverage multidisciplinary nature of Insider Threat and identify metrics from:
  - Human Resources
  - Legal
  - Physical Security
  - Information Technology
  - Information Security
- Contextualize Insider Threat Program activities within existing metrics frameworks – whether open source or proprietary

ITIL Framework for Metrics – Insider Threat Examples

Technology

- Impact or lack thereof of employee monitoring programs on performance
- Availability of data sources for processing by Insider Threat program

Process

- Number of capability gaps identified or improved
- Average incident resolution time per month
- Number of inquiries completed per month

Service

- Management feedback or engagement with Insider Threat program
- Cost of inquiry
- Time to complete an inquiry

More information on ITIL can be found at: https://www.itlibrary.org/

Other Metrics to Consider

Coverage

- percentage of systems covered by a host-based user activity monitoring system
- process reviews
- gap assessments
  - Increasing data insights where there was previously no visibility.
  - Identifying gaps in administrative, physical and technical controls.

Latency

- average time between malicious activity and discovery by insider threat team
- risk avoidance and ability to proactively identify any issues where the risk can be mitigated

Compliance

- percentage of recommended / required (NIST SP 800-53, NITTF Minimum Standards) controls implemented
- pre-employment screening
- code of conduct
- Data Loss Prevention (DLP)
- mandatory vacation policies
- investigation teams

Impact

- number of incidents identified or prevented
- incidents that result in action
  - e.g., escalated to management or law enforcement, leads, inquiries, investigations, cases closed
- reduction in time to resolve allegations
- reduction in number of incidents over time
- value of any data targeted for exfiltration, or documents / IP recovered
  - aggregate of estimated value per incident in a reporting period
  - multiply average incident by value to estimate financial impact for future incidents
- 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

Measures of Effectiveness

Qualitative

- Security culture
- Training and awareness leading to increased reporting
- Identification of broken processes
- Case study
- Incident severity / criticality

Quantitative

- Referrals and reports from staff
- Investigations
- Incidents detected
- Incidents referred to law enforcement
- Sites blocked
- Assets recovered
- Loss prevented

Time Management Matrix

	Urgent	Not Urgent
Important	**Quadrant I - Manage** • Crisis • Pressing problems • Deadline-driven projects, meetings, preparations	**Quadrant II – Focus** • Preparation • Prevention • Values clarification • Planning • Relationship building
Not Important	**Quadrant III – Avoid** • Interruptions, some phone calls • Some mail, some reports • Many proximate pressing matters • Many popular activities	**Quadrant IV – Limit** • Trivia, busywork • Junk mail • Some phone calls • Time wasters • "Escape" activities

- Where is time being spent by analysts? At the program management level?
- Are you able to move from *Manage* to *Focus* activities?

7 Metrics to Prove the Value of an Insider Threat Program

- **Cases opened:** Number and types of cases reviewed by the program
- **Internal requests for information:** Number and types of RFIs to organizational stakeholders
- **Internal escalation and triage:** Number and types of cases escalated and triaged within the organization
- **External escalation and triage:** Number and types of referrals to external law enforcement agencies
- **Risk mitigation actions:** Number and type of risk mitigating actions
- **Documents retrieved:** Number of document prevents from leaving a secure environment
- **Investigative productivity:** Average reduction in investigative timelines

From *Insider Threat: Prevention, Detection, Mitigation, and Deterrence* by Michael Gelles

What's in a False Positive?

High false positive rates can potentially

- waste analyst / investigative resources
- alienate employees
- exacerbate threats
- reduce morale
- repel good employees
- increase claims of privacy violations and lawsuits
- erode support for the InTP across the organization and among senior leadership

Moore et al. "Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls", available online at http://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_446379.pdf

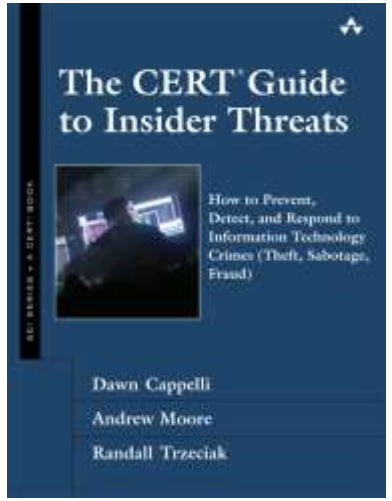
Questions for Consideration

- What resources have you found valuable in developing metrics?
  - Were these resources internal or external to your organization?
  - Were the external resources open source or proprietary?
- What kinds of metrics has your organization used in the last 12 months?
  - What type of use case was it used for?
  - Was the metric reliable? Valuable? Useful?
- What metrics failed to make an impact on stakeholders?
- How are measures for Insider Threat success or value different from those used for a Security Operations Center (SOC)?
  - How could they be the same?
  - What lessons learned for developing SOC metrics can be used for Insider Threat?
- To what extent could (or should) other organizational units help to demonstrate the value of the Insider Threat program?

NITC Resource Highlights

- 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

NTIC Publications and References



Collins, M., Theis, M., Trzeciak, R. F., Strozer, J., Clark, J., Costa, D., Cassidy, T., Albrethsen, M., & Moore, A. P. (2016). Common Sense Guide to Mitigating Insider Threats (5th Ed.). Pittsburgh: Software Engineering Institute.

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley Professional.

Moore, Andrew; Savinda, Jeff; Monaco, Elizabeth; Moyes, Jamie; Rousseau, Denise; Perl, Samuel; Cowley, Jennifer; Collins, Matthew; Cassidy, Tracy; VanHoudnos, Nathan; Buttles-Valdez, Palma; Bauer, Daniel; & Parshall, Allison. The Critical Role of Positive Incentives for Reducing Insider Threats. CMU/SEI-2016-TR-014. Software Engineering Institute, Carnegie Mellon University. 2016.

For More Information

National Insider Threat Center	http://www.cert.org/insider-threat/
National Insider Threat Center Email	insider-threat-feedback@cert.org
National Insider Threat Center Blog	http://insights.sei.cmu.edu/insider-threat/
SEI Digital Library	https://resources.sei.cmu.edu/library/

Contact Information

Sarah Miller

Insider Threat Researcher

CERT National Insider Threat Center

Email: semiller@cert.org

Software Engineering Institute

Carnegie Mellon University

4500 Fifth Avenue

Pittsburgh, PA 15213-3890