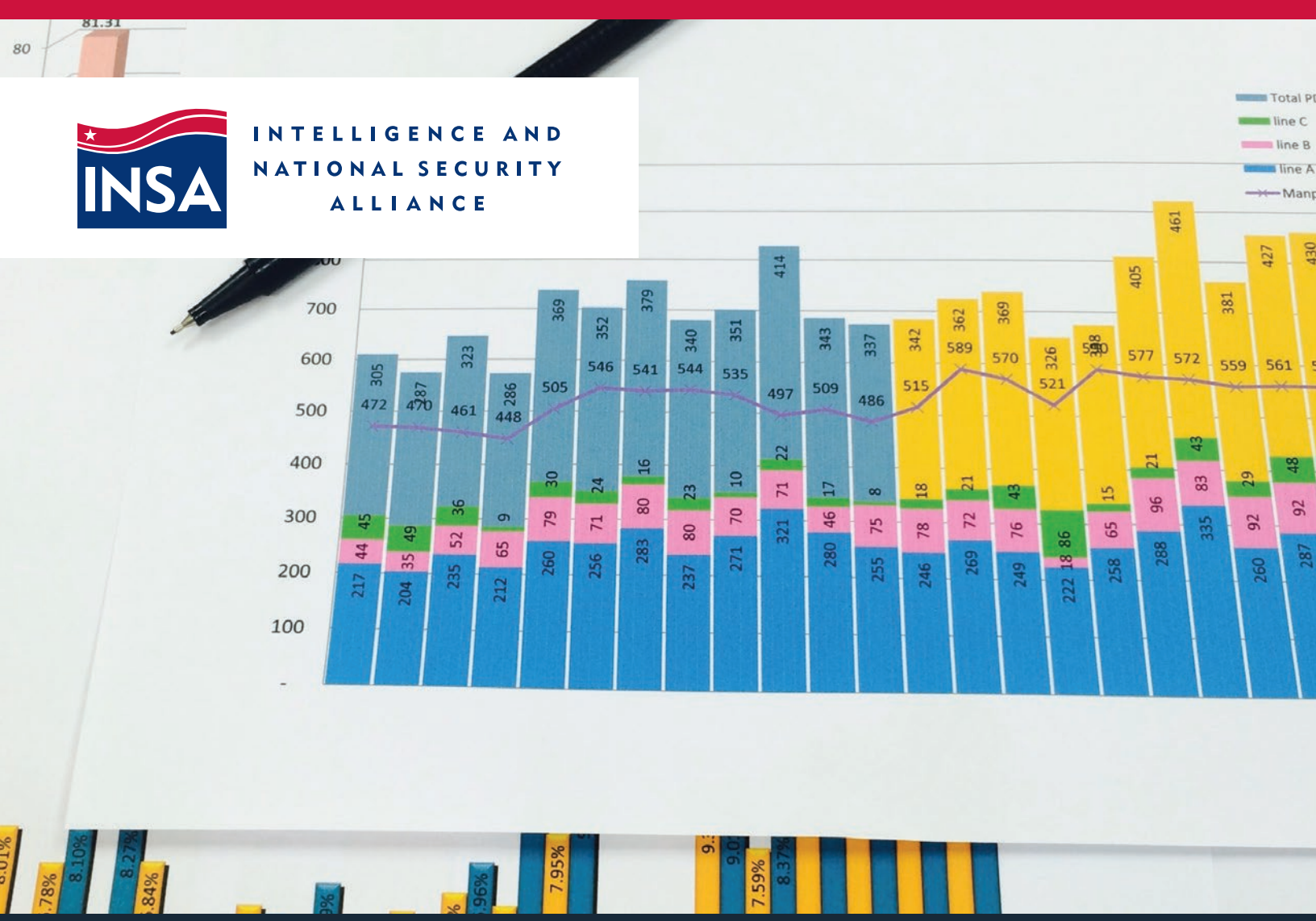
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE



SEPTEMBER 2022

Measuring the Effectiveness of Insider Threat Programs

Presented by

INSA'S INSIDER THREAT SUBCOMMITTEE

Building a Stronger Intelligence Community

EXECUTIVE SUMMARY

Building effective ways to measure the success of an insider threat program (InTP) is important to assess whether and to what extent the program has an impact. Moreover, specific metrics can help to justify the program to leadership resulting in continued funding, resources, and support. Unfortunately, "magic metrics" do not exist. The effective measurement of an InTP depends on an organization's unique set of requirements and its desired business outcomes.

Metrics should reflect both the program's maturity and "What's Important Now" to the organization. People and organizations fall into the trap of counting and measuring activities that don't support decision-making, such as the number of record checks. Metrics should give reasons for people to support and invest in the program as well as drive positive results and behaviors. Investing time early in a program's development to determine short- and long-term objectives makes it easier to identify appropriate metrics for achieving those objectives, which in turn enable program managers to demonstrate the value of their program to leadership.

INTRODUCTION

Insider Threat Programs (InTPs) are complex, enterprise-wide functions with program objectives and stakeholders that vary from organization to organization depending on size, industry, complexity, legal jurisdiction, etc. Like other security-related programs, INTPS are typically overhead cost centers rather than profit-generating businesses (unless the organization leverages their InTP as a service offering for clients). Establishing appropriate objectives and performance metrics supports business justifications for resources (budget and personnel) and ensures sustained buy-in and support from senior leadership and other key internal stakeholders. However, many organizations struggle to develop metrics that show the actual value of their InTPs—specifically, measures of effectiveness (MOE) and return-on-investment (ROI).

Clear metrics that are tied to program objectives help to:

- Align InTP operations with the business objectives of the organization
- Demonstrate that the InTP is achieving its intended purpose
- Inform InTP stakeholders of both successes and challenges
- Optimize InTP performance over time
- Achieve compliance with applicable laws, regulations, and policies
- Identify areas to increase security awareness and training efforts
- Identify vulnerabilities and gaps in other organizational policies/programs

“Establishing appropriate objectives and performance metrics supports business justifications for resources and ensures sustained buy-in and support from senior leadership and other key internal stakeholders.

CHALLENGES TO MEASURING InTP EFFECTIVENESS

InTPs generally rely heavily on log data and user activity monitoring. More mature programs demonstrate a greater combined emphasis on user activity monitoring, forensic tools, and user behavioral analytics. However, a survey created by Henderson & Cavalancia (2019) found that organizations often struggle to leverage user activity data to develop proactive responses to potential insider threats. In describing program effectiveness, program managers’ responses ranged from “Nonexistent Program” (two percent of the survey’s organizations have no program in place) to “Optimized,” where an organization’s InTP is dynamic and responsive, employing comprehensive monitoring of all employees using tools and techniques that seek to identify both unintentional and malicious insider threats.

Survey respondents managing Optimized Programs (19 percent of all programs) characterized their activities as follows:

- 56 percent of organizations performed monitoring of all employees;
- 37 percent of organizations engaged in "Predictive" monitoring practices;
- 23 percent of organizations used a "Proactive" approach that monitors individuals considered to be at high risk for malicious insider threats; and
- 16 percent of InTPs are "Reactive," responding only after an incident occurs.[1]

In an informal survey conducted by INSA to learn how or whether InTP practitioners measure their programs' effectiveness, only 32 percent of survey respondents said they could determine the effectiveness of their program.[2] More than half of the respondents claimed they were "working on it," and the rest were not sure where to start. These survey responses indicate that organizations need to increase their understanding of the importance of MoEs and ROIs for their programs, and that InTP managers need to learn how to develop such metrics.

INSA Survey: What challenges do you face in measuring the effectiveness of your InTP?

"What should we be doing? How do you determine if it's effective? We are trying, but I know other small firms are struggling also."

"Need a better way to track the incidents."

"My company does not give me the time or the resources to effectively manage the InTP the way it should be. They see it as a compliance issue of having a plan and don't really believe we need anything further."

"With a small company there are very little active cases/incidents and even less willingness to do anything beyond the required training."

What challenges do you face in measuring ROI of your InTP?

"ROI is not considered. If it is a government requirement, we do it. If it is a best practice, but not required, we don't do it."

"We have no way to measure this. Hopefully the IT training is reminding people to stay out of trouble and report but we've had no reports."

"No results currently obtained to measure ROI, no active processes to detect Insider Threat activity."

"Don't know how to establish metrics to measure against."

TYPES OF MEASUREMENTS

OPERATIONS-BASED MEASUREMENTS

"Operations-Based Measurements" measure processes or activities and are fundamental for measuring process improvement through analytic frameworks such as Lean Six Sigma's DMAIC (Define, Measure, Analyze, Improve and Control) or SIPOC (Suppliers, Inputs, Process, Outputs, and Customers).[3] Operational measures will equip program managers to convey impact by measuring inputs ("level of effort") and eventual ROI.

Operations-based measurements are most efficiently calculated when they are built into the processes themselves. For example, if the number of investigations is identified as a useful operations-based measurement, it should be measured by the system used to generate leads or by a case management system. When operations-based measurements are generated and collected through an instrumented fashion, program managers have greater confidence in their accuracy and are more likely to use them. However, when operational measurements require manual calculations, they are frequently avoided because they are more prone to errors and are perceived to cost more in calculating than they are worth. Accordingly, processes and workflows should be designed with operations-based measurements in mind.

Examples of operations-based measurements include:

- Number of cases generated
- (Average) length of time to detection
- Number of cases generated by detection capability
- (Average) length of time to case closure
- Number of cases assigned to an investigator
- Number of investigators assigned to a case

Operational measures can also be combined or analyzed together. For example, analyzing the length of time to case closure combined with the number of investigators assigned to the case may give a more accurate indication of "level of effort."

PROGRAMMATIC-BASED MEASUREMENTS

InTP managers should not only concern themselves with the operations performance of the program but also collect programmatic-based metrics, which assess and validate the InTP's achievement of its intended purpose. Similarly, metrics can and should be collected to validate the InTP's alignment with the organization's broader, strategic objectives. This planning process begins by drawing on clear organizational objectives, aligning them to program objectives and desired outcomes, and developing metrics that measure them.

As highlighted by the Defense Security Service (now the Defense Counterintelligence and Security Agency) in Industrial Security Letter ISL 2016-02, a clear program objective may be "to detect, deter, and mitigate insider threats."[4] Programmatic-based measurements should align with evidence that demonstrates effectiveness in "deterrence," "detection," as well as "mitigation." Aligning metrics along these programmatic objectives will not only validate the effectiveness of the program but provide objective measures to identify deficiencies and/or focus programmatic enhancements and investments.

Similarly, InTPs all reside within a broader organizational construct which necessarily has its own higher-level objectives. A program which is effective in contributing value to the organization should have metrics that align with those organizational objectives. For example, an InTP that resides in an organization's Office of General Counsel might be cognizant of a goal of "enhancing protection of intellectual property rights" and identify measures to ensure its contribution to this outcome. Likewise, a program aligned with the Chief Information Officer might identify programmatic metrics which validate the program's value in "enhancing the protection of critical IT infrastructure."

WHERE DO YOU START

The answer to this question, like most aspects of Insider Threat, is not a one-size-fits-all solution. A better way to look at this question may not be "where DO I start" but "where CAN I start."

Too often programs attempt to provide metrics to leadership prematurely. If a program sets out to report the total number of insider threats detected by technical tools but doesn't have those tools fully deployed or implemented, the metric won't provide any value. Indeed, managers may undermine their goals by promising achievements that the program simply isn't set up to produce.

While it's desirable to achieve production metrics that reflect performance (e.g.,"tools detected X incidents, which led to Y inquiries, which led to Z investigations"), it's important to place them into the process when the program is ready to support it. Without a fully deployed detection solution, attempting to provide that metric would most likely generate updates to leadership saying, "We've accomplished nothing." So, to answer the question, "Where CAN I start?", identify the measurable value the program can provide today, while giving continued updates on where the program is headed in the future.

While detection tools may take time to fully implement, a hub may be established and provide significant value in enabling multiple business lines to respond to an insider threat indicator. Even without a full deployment of insider threat tools, InTPs may be able to provide one-off monitoring support to an investigation being undertaken by another part of the organization. Finally, it is useful to track progress of tool deployments, such as the use of roll-out numbers on monitored endpoints or datasets being acquired for a behavioral analytic system.

IMPACT OF METRICS ON InTPS

Metrics should enable the program manager to tell a story in both an operational and programmatic context. Operationally, that story may be that demand has outpaced capacity or that through an investment in technology, capacity has been able to finally keep up with demand. Programmatically, the story may be that strategic risk has been reduced in the areas identified as most critical to the executive leadership team. Not all questions can be proven with metrics (e.g., how many incidents were prevented); however, a comprehensive assortment of metrics will likely enable program managers to speak to indicators of reduced risk (e.g., how many vulnerabilities were reduced).

WHERE DO WE GET THE DATA FOR METRICS?

For Operations-Based Measurements, detection and analytic tools such as User Activity Monitoring (UAM) and User/Entity Behavior Analytics or case management systems offer an ideal mechanism to collect data and calculate metrics. That said, even less mature programs can use basic tools such as spreadsheets to calculate metrics for management of activities and outcomes.

When developing measures programmatically, it is important to measure outcome and the current state/status of the program. Programmatic-Based Measurements will likely require more deliberate planning and may be difficult to incorporate into business processes and activities. However, deliberate planning will enable the astute program manager to document these outcomes.

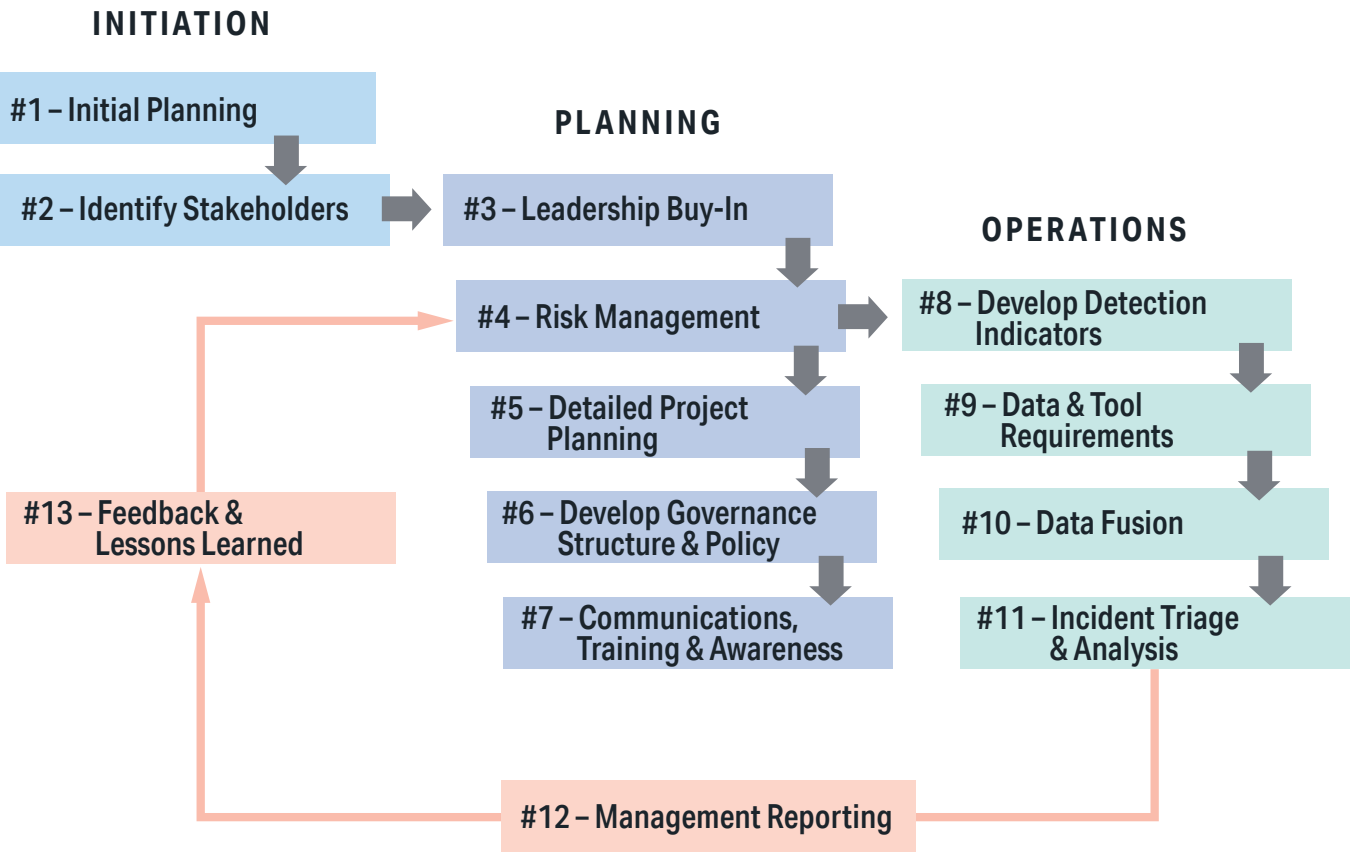
CHOOSING THE RIGHT METRICS FOR YOUR InTPs

There is no shortage of potential reportable data in an InTP: the number of UAM events, analyst level of effort, inquiries opened and closed, the dollar value of recovered intellectual property, the status of audit findings, etc. The list is endless. The "right" metrics for an InTP must be determined by program managers based on internal priorities. There may be temptation to recycle metrics the program manager has used at a previous employer. The program stakeholders sitting around the conference room table may have a long list of "important" things they want to measure, without a clear set of reasons for their favorite statistics. With almost unlimited data and no clear reason to measure any of it, the organization risks falling into the trap of counting and measuring things that don't help it make decisions and that don't measure progress towards program objectives.

InTP metrics should:

- Be relevant to a program's stage of development
- Align to current program objectives
- Guide decision-making
- Help identify unintended consequences of program initiatives
- Contribute to sustaining the support of senior leadership for program activities

Choosing the right metrics begins with determining "what's important now." As described in INSA's 2017 InTP Roadmap,[5] from which the below figure is derived, programs mature and progress from initiation, to planning, operations, and continuous improvement.



Metrics guiding the organization through its program initiation stage are different from those seeking to improve its effectiveness after several years of implementation. Metrics must be closely coupled to the process used to establish short- and long-term program goals. For example, is the program hiring analysts or working to raise the technical competence of the analyst team and its application of the selected threat model? The maturation distance between these two points makes choosing one analyst metric impossible, and metrics must certainly evolve over time. Therefore, the program should begin with its defined and prioritized near- and long-term objectives and its theory of cause and effect to assess the impact of program initiatives.

Building and operating InTPs introduces change to the organization. Change has consequences, good and bad, so organizations should identify opportunities to obtain metrics that will help to detect unintended consequences.[6] Examples of unintended consequences include interference with legitimate whistleblowing activities, adverse impact to employer-employee relationships, or misuse of technical capabilities.

Finally, the program manager should consider whether program metrics will contribute to sustaining the support of senior management in the program. If a program's metrics are difficult to understand or appreciate, senior management may fall back on time-tested business metrics that indicate whether your program is sticking to timelines and budgets.

“When planning metrics... you should first and foremost consider how you will count or collect the data necessary to fulfill the metric, as the metric is only as good as the data collected.

EXAMPLE METRICS

Management thinker Peter Drucker is often quoted as saying, “What gets measured gets managed.” You cannot determine your program's effectiveness until you define “effectiveness” and take steps to measure it. In the case of InTPs, Drucker's dogma translates to, “You can't measure what you don't count.” When planning metrics, of which there are many types, you should first and foremost consider how you will count or collect the data necessary to fulfill the metric, as the metric is only as good as the data collected. Programs should not become frustrated or mired in indecision because data is not currently available for the most ideal metric. Therefore, you may need to pass over an “ideal metric” for an “available metric.” It is okay to focus, at least initially, on metrics for which data is currently available, with the goal of expanding and maturing metrics over time. Examples of representative metrics include counting the numbers of InT reports and tracking events generated by InT products (a detailed list in provided in the Appendix).

METRICS IN ACTION – Insider Threat reports generated by incident type

The InTP for the ABC Corporation captures metrics for the number of insider threat reports generated by incident type by week, quarter, and year. That metric is reviewed weekly by the InTP manager and reported to executive leadership quarterly and the Board of Directors yearly. By tracking this metric, the InTP manager identified a concerning upward trend in the number of cases opened between last quarter and this quarter for removable media device connection attempts to corporate assets. An ABC corporate policy states that no employee can connect removable media devices to corporate assets. By identifying the upward trend in unauthorized connection attempts, the InTP manager worked with the stakeholder responsible for cybersecurity and insider threat training to add training to increase awareness related to the removable media corporate policy and the consequences for violating that policy. Further review of the Acceptable Use Policy (AUP) addressing removable media determined that the AUP is unclear and lacks reference to the consequences of violating the policy. ABC Corporation stakeholders then updated the AUP to address the deficiencies and launched a campaign to make employees aware of the policy updates. Over the next several quarters, the InTP saw a 25% decrease in removable media connection attempts, and the insider threat program manager reported the downward trend and positive impact the InTP had in this situation to executive leadership at the quarterly briefing and the Board of Directors at the yearly briefing.

In this example, by collecting and baselining metrics related to the number of reports generated by incident type, the corporation realized the positive effect of its InTP from a single metric. As a result of the InTP identifying and reporting a concerning trend, the organization's stakeholders responded by updating the AUP and creating a training and awareness campaign that reduced the risk of unauthorized removable media connection attempts to the organization.

METRICS IN ACTION – Mean Time to Resolution

The InTP at the ABC Corporation has been active for some time. Their detection technology is fully deployed and maintains mature metrics. The Program reports quarterly to the InTP Manager, who in turn reports to the Board of Directors, the total time and effort taken to respond and resolve a potential insider threat incident. Over the past two quarters the InTP Manager has identified a noticeable downward trend in the time it takes for the Program to effectively work a potential issue to resolution. Additional metrics also show the program has received a 45% increase in referrals, significantly increasing its workload. The InTP manager uses this information to lobby the Board for additional resources.

CONCLUSION

Measuring the effectiveness of an InTP is vital to ensuring sustained buy-in and support from senior leadership and other key stakeholders. To be effective, InTPs must be equipped with the resources and practices necessary to identify internal and external variables that help predict the organization's risk from insiders. Recording precise metrics will help organizations understand if their actions were sufficient to detect and mitigate insider threats.

InTPs must evolve and adapt to changing variables in the work environment. Once an organization identifies the MOEs they will use, these metrics should be reviewed on a routine basis to show where the InTP is improving the organization's security posture and where there is still room for improvement. Routinely measuring InTP effectiveness will enable benchmarking – providing the necessary input to answer questions such as "how well are we doing at mitigating insider threats relative to our peers?" Over time, measurements will provide a comprehensive picture of how the program responds to ever-changing workplace environments.

APPENDIX

Examples of Operations- and Program-Based Metrics for Measuring the Effectiveness of Insider Threat Programs

METRICS	EXPLANATION	FREQUENCY & STAKEHOLDERS	MEASUREMENT TYPE
Insider threat reports generated by source	Track the number of insider threat reports generated by the source of detection/ notification to show which mechanisms are working as intended or not working as intended. This could happen in several ways, including an insider threat product, tip line, business unit, or another employee.	Insider Threat Program Manager (Weekly)	Operations
Insider threat reports generated by analyst	Helps measure overall level of effort and gauge productivity, workload, and future staffing needs	Insider Threat Program Manager (Weekly)	Operations
Events generated by insider threat product	An event is something that is generated for review from an insider threat product when something potentially concerning is detected. Tracking this metric helps to identify the need to tune noisy products and manage the workload of the analysts.	Insider Threat Program Manager (Weekly)	Operations
Events reviewed per analyst	An event is something that is generated for review from an insider threat product when something potentially concerning is detected. Tracking the number of events viewed by an analyst helps understand analyst productivity. It could be an early indicator of future staffing needs or the need to assess for process improvements to aid analyst efficiency.	Insider Threat Program Manager (Weekly)	Operations
Average risk score per employee	Relevant if using a UEBA product or other risk rating tools that assess and assign an overall (dynamic) risk score to each employee. Identifying averages across the organization and/or business units will help identify trends and/or used to tune tools	Insider Threat Program Manager (Weekly) Executive Leadership (Quarterly)	Operations
UAM policy/event rate	Most UAM products create events based on policy triggers. Understanding the rate (number of events per capita) of each policy/event will inform whether risk tolerances and/or thresholds should be adjusted to avoid "false positives."	Insider Threat Program Manager (Weekly)	Operations
Insider threat reports generated by business unit	Tracking the number of insider threat reports generated by business unit helps identify organizational vulnerabilities. Incidents per business unit may indicate an increase in risk or, coupled with other metrics, may indicate the effectiveness of other initiatives like training and education.	Insider Threat Program Manager (Quarterly) Executive Leadership (Quarterly)	Program

METRICS	EXPLANATION	FREQUENCY & STAKEHOLDERS	MEASUREMENT TYPE
Inquiries made to the insider threat program by BU	An inquiry is when a part of the organization requests support or information from the insider threat program. This could be a request from legal or human resources to support an investigation they are running and want to leverage capabilities within the insider threat program. The metric shows how often the insider threat program is leveraged and by which BUs.	Insider Threat Program Manager (Quarterly) Executive Leadership (Quarterly)	Program
Employee Assistance Program (EAP) referrals generated from the insider threat program	An employee is an organization's greatest asset. When the insider threat program helps identify employees who may need the EAP and notifies the appropriate stakeholder that should be tracked and reported.	Insider Threat Program Manager (Weekly) Executive Leadership (Quarterly) Board of Directors (Yearly)	Program
Sensitivity of materials mishandled/exfiltrated	This is the total number of files/documents/etc. that were detected as mishandled and/or exfiltrated by information handling caveats (e.g., FOUO, CUI, Internal Use Only) and/or sensitivity levels (e.g., low sensitivity, moderate sensitivity, etc.). In the context of other metrics, this will enable a root-cause analysis of detection gaps, vulnerabilities, and/or impact of investigations.	Insider Threat Program Manager (Quarterly) Executive Leadership (Quarterly) Board of Directors (Yearly)	Program
Impact of materials mishandled/exfiltrated	This is the compliance impact and/or monetary value of the information in the materials identified as being mishandled or exfiltrated. This is valuable in assessing programmatic value and impact, which can be measured and articulated in a number of different means such as "return on investment."	Insider Threat Program Manager (Quarterly) Executive Leadership (Quarterly) Board of Directors (Yearly)	Program
Insider threat awareness training	Tracking frequency and dates of training can help analyze in concert with other metrics to identify whether training is having an impact on the occurrence of events and/or the reporting of events.	Insider Threat Program Manager (Quarterly) Executive Leadership (Quarterly) Board of Directors (Yearly)	Program
Active insider threat investigations	The number of active insider threat cases open is used to gauge program personnel's overall level of effort and capacity. It can also be an indicator of a broken process if a large number of cases remain open for an extended period.	Insider Threat Program Manager (Weekly)	Program & Operations

METRICS	EXPLANATION	FREQUENCY & STAKEHOLDERS	MEASUREMENT TYPE
Mean time to detect the incident	This is the amount of time to detect an incident averaged across all incidents. This will aid in assessing the effectiveness of tools and/or gaps in detection through root-cause analysis.	Insider Threat Program Manager (Quarterly) Executive Leadership (Quarterly)	Program & Operations
Mean time to respond to the incident	This is the amount of time to respond to an event after detection averaged across all incidents. This will aid in identifying inefficient processes and/or lack of capacity (e.g., personnel).	Insider Threat Program Manager (Quarterly) Executive Leadership (Quarterly)	Program & Operations
Mean time to resolve	This is the amount of time to resolve an incident averaged across all incidents. This will aid in identifying inefficient processes and/or lack of capacity (e.g., personnel).	Insider Threat Program Manager (Quarterly) Executive Leadership (Quarterly)	Program & Operations
AVG insider threat case length	It helps to understand the average length of time it takes to close a case once it's opened. It helps to identify inefficiencies and staffing needs.	Insider Threat Program Manager (Weekly) Executive Leadership (Quarterly)	Program & Operations
Insider threat report referred by stakeholder	When an insider threat report is generated based on the incident response procedures, that report is sent to the corresponding stakeholder for further action. Tracking the number of reports sent to each stakeholder for further action allows the insider threat program to identify trends.	Insider Threat Program Manager (Weekly) Executive Leadership (Quarterly)	Program & Operations
Reports generated by incident type	Tracking the number of reports generated by incident type helps identify trends, areas of concern, and how often different types of incidents are happening within the organization to enable root-cause analysis and identification of strategic mitigations.	Insider Threat Program Manager (Weekly) Executive Leadership (Quarterly)	Program & Operations

REFERENCES

[1] *Henderson, J., & Cavalancia, N. (2019). 2019 InTP Maturity Model Report.*

[2] *At https://cdn2.hubspot.net/hubfs/5260286/PDFs/Whitepapers/insider-threat-maturity-report-2019.pdf.*

[3] *IBM. (2021). Cost of a Data Breach Report 2021. At https://www.ibm.com/security/data-breach.*

[4] *Kirkpatrick, D. (1998). Evaluating Training Programs: The Four Levels. 2nd Edition. San Francisco: Berrett-Koehier.*

[5] *Miller, S. (2018, January 17). 2017 U.S. State of Cybercrime Highlights. At Insider Threat Blog: https://insights.sei.cmu.edu/insider-threat/2018/01/2017-us-state-of-cybercrime-highlights.html.*

[6] *Retruster. (2019). 2019 Phishing Statistics and Email Fraud Statistics. At https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html.*

[7] *Verizon. (2019). 2019 Data Breach Investigations Report. At https://enterprise.verizon.com/resources/reports/dbir/.*

[8] *Poneman Institute and IBM Security. (2020) Cost of Insider Threats: Global Report 2020. At https://www.ibm.com/downloads/cas/LQZ4RONE.*

[9] *National Insider Threat Task Force (NITTF), Insider Threat Program Maturity Framework, November 1, 2018. At https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf.*

[10] *Campbell, G (2014). Measures and Metrics in Corporate Security. 2nd Edition.*

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Sue Steinke, Peraton; *Insider Threat Subcommittee Chair*

Julie Coonce, Premise; *Insider Threat Subcommittee Vice Chair*

Julie Ard, *Noblis*

Marcus Carpenter

Dan Costa, *Carnegie Mellon University SEI*

Michael Crouse, *Forcepoint*

Andrew Distler, *Forcepoint*

Frank L. Greitzer, *PsyberAnalytix*

Josh Massey, *MITRE*

J.T. Mendoza

Mike Miller, *Forcepoint*

Dan Velez, *Forcepoint*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor,
Director of Communications and Policy

Cassie Crotty, *Intern*

Emma McCaleb, *Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S INSIDER THREAT SUBCOMMITTEE

INSA's Insider Threat Subcommittee researches, discusses, analyzes, and assesses counterintelligence and insider threat issues that affect government agencies, cleared contractors, and other public and private sector organizations. The Subcommittee works to enhance the effectiveness, efficiency, and security of government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors.

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

Building a Stronger Intelligence Community