NDIA

Insider Threat Workshop

LEARNING OBJECTIVES:

- Learn how to overlay your Insider Threat program onto existing security programs.
- Examine behavioral risk indicators & identify organizational and situational triggers for the violent & non-violent insider threat.
- Develop your Strategic Goals and Concept of Operational Plan.
- Learn the psychometric approach for designing metrics, how to analyze metrics, & techniques for repurposing existing metrics to best fit your organization's needs.

May 17-18, 2018
NDIA | Scottsdale, AZ

Workshop Highlights:

Develop an Operational Strategic Plan

Identify characteristics of the Insider Threat Program elements required to meet organizational expectations and develop a Concept of Operations. Learn how to leverage your existing internal organizational policies and infrastructure to build an efficient program.

Integrated Behavioral Modeling

Learn what a "behaviorally-focused" Insider Threat Program entails and discuss how to use criterion data to identify behavioral indicators and detect anomalies. Take the behaviors learned to develop effective Performance Measures, then identify and mitigate Insiders before they become a threat.

Effectively Collaborate to Build and Maintain an Insider Threat Program

Learn how to build an Insider Threat Working Group and elicit support from law enforcement and federal officials to better protect information and assets. Team exercises are used to reinforce skills learned and provide collegial interaction.

Communicate with Senior Management and Gain Buy-in for an Insider Threat Program

There are three categories to consider when building a security metric: the psychometric principles in the design; the security considerations; and the value to senior management. Learn how to build a valuable security metric and assess the continuing strength of the metric through application of the Security Metrics Evaluation Tool (Security MET).

Workshop Breakdown:

This two-day program is designed to help organizations build the essential components of an effective Insider Threat Program using modern organizational theory, analytic techniques and measures that exceed federal guidelines for 2018.

Learn how to evolve your current security program into a converged management structure that will identify and deter individuals who pose both violent and non-violent threats. Learn the skills and procedures required to identify factors that are critical to shaping a comprehensive Insider Threat Program.

Real case studies are used to show how work behavior can reveal early signs of a potential insider threat, to examine the potential risk indicators and to reveal how organizations can be structured to best detect and deter the insider threat.

Insider Threat Education and Training

Understand the importance of organizational training and education to senior management, security staff, and the entire workforce. Learn how to effectively employ your Insider Threat Working Group to provide training and awareness to a diverse workforce.

Integrate an Insider Threat Program with Enterprise Security Risk Management

Learn to identify and apply protection specifications as part of an Insider Threat program. Understand how to coordinate the economical use of resources to identify, assess, and prioritize the risk associated with specified assets within the scope of an Insider Threat program.

Building a Strategic Plan and CONOPS

Using an outline, learn the stepwise approach in building a security strategic plan and Concepts of Organization (CONOPS) guide for your organization. Learn the practical approaches in developing and presenting your ideas in an effective and compelling approach to senior management.

Insider Threat Structure

Learn the nine components of an effective Insider Threat Program. Discover how to repurpose existing assets and metrics to develop a demonstrable Return on Security Investments (Security ROI). Learn how to use the Convergence model to bring diverse elements of your organization to work together against the Insider.

In addition:

- Understand the requirements for designing, developing, coordinating, and continuously evaluating an integrated insider threat program.
- Learn the methodologies used to identify insiders, individual motivators and corporate triggers.
- Examine behavioral risk indicators and identify organizational and situational triggers for the violent and non-violent insider threat.
- Learn mitigation techniques for internal alerting, reporting, collecting, storing, and evaluating data relevant to insider threat indicators.
- Review the laws, regulations, civil liberties, and policies, collecting, storing, and evaluating data relevant to insider threat indicators.
- Learn and practice the psychometric approach to building metrics; how to analyze existing measures; and how to re-purpose existing metrics from across the organization for your needs.

Daniel A.McGarvey

Mr. McGarvey, a retired Defense Intelligence Senior Executive Service officer, has over 40 years of in-depth experience managing and directing national and international programs requiring sensitive compartmented information and special access in government and industry. Mr. McGarvey is an experienced program director: he rebuilt the security infrastructure for the Department of the Air Force. Further, he redesigned the corporate security management structure at the AF Secretary Staff level. This design is used by the Security, Nuclear and Space Communities and has been adopted by the Department of Defense as the standard security governance structure. Mr. McGarvey has developed and executed a comprehensive protection program for the Secretary of the Air Force to organize, train and equip almost 6,000 civilian and military security personnel worldwide.

His current responsibilities include providing executive consulting and training for the design and implementation of Security and Counterintelligence programs for government and industry. He is a member of the National Counterintelligence Executive/National Counterintelligence and Security Center (NCIX/NCSC) Industry Security Advisory Group. He is also the behavioral analytics lead for the Intelligence and National Security Alliance/Security Policy Reform Council (INSA/SPRC) Insider Threat Working Group, and member of the National Defense Industrial Association (NDIA) Industrial Security Division. Mr. McGarvey is an industry representative to the National Industrial Security Policy Advisory Committee (NISPAC). Further, as an American Society for Industrial Security (ASIS) International member, he was the former Chair of the Chief Security Officer (CSO) Leadership Development Committee (LDC), and Chair of the Defense & Intelligence Council (D&IC).
He is a Senior Principal Business Process Analyst for Alion Science and Technology

His current co-authored paper: Assessing the Mind of the Malicious Insider: using a behavioral model and data analytics to improve Continuous Evaluation will be provided at the workshop.

His current papers in final draft include: The Personnel Security Adjudicative Guidelines and Insider Threat Behavioral Models: an evolutionary path to the Trusted Employee and a coauthored paper on: An Assessment of Data Analytics Techniques for Insider Threat Programs will be provided as well.

NDIA

The National Defense Industrial Association (NDIA) is America's leading defense industry association promoting national security. NDIA provides a legal and ethical forum for the exchange of information between industry and government on national security issues. NDIA members foster the development of the most innovative and superior equipment, training and support for warfighters and first responders through our divisions, local chapters, affiliated associations and events.