Contribution ID: **538** Type: **Interactive Content Presentation**

Preliminary Results from Invoking Artificial Neural Networks to Measure Insider Threat Mitigation

Insider threat mitigation programs have traditionally focused on preventative and protective measures to mitigate insider threats (and resulting malicious acts) to nuclear facilities. Preventive measures—including pre-employment background investigations—are those implemented before trusted access is provided to nuclear facilities. Protective measures—including the two-person rule for accessing more sensitive facility locations—are those implemented after trusted access is provided. These approaches tend to focus on identifying and deterring the problematic or malevolent behaviors of individuals instead of evaluating collective behaviors observed in the facilities. This approach has resulted in an overreliance on generic job tasks analysis and detection of aberrant behavior that does not account for patterns of workplace behavior, ignores facility recovery operations, and lacks adequate measures of mitigation effectiveness.

In response, research from across the government and private sector has hypothesized ways to utilize empirical data from increasingly networked security and facility "health-monitoring"systems to improve, and even automate, portions of insider threat mitigation programs. More specifically, this research argues that a better understanding of workplace dynamics will improve the ability to identify, detect, and forecast the potential for a successful insider threat action. This type of approach better integrates workplace behavior-related insights into traditional insider threat mitigation programs. These advances, while important to the long-term success of insider threat mitigation programs, are based on differentiating between malicious intent and natural "organizational evolution"to explain observed anomalies in collective workplace dynamics, trends, and patterns.

To better understand how these patterns impact insider threat mitigation efforts, a collaborative research project between the U.S. National Nuclear Security Administration's International Nuclear Security Program (NNSA/INS), Sandia National Laboratories (Sandia), and the University of Texas at Austin (UT-Austin) collected empirical data on work patterns at the Nuclear Engineering Teaching Laboratory (NETL)—a TRIGA MARK II research reactor facility—at UT-Austin. Signals collected from door access readers, video surveillance, area radiation monitors, and personnel radiation detection portals were combined with a commercially available software tool from ReconaSense to quantitatively describe insider threat potential and evaluate mitigation effectiveness. More specifically, this project leveraged the ability of artificial neural networks to synthesize—and learn from—disparate data sources (e.g., card access readers) for perform anomaly detection. This project also applied resilience algorithms to describe insider threat mitigations in terms of well-known theories of organizational behavior. This paper summarizes a new approach for understanding, identifying and evaluating insider threats—including a more advanced evaluation framework and set of measures—capable of improving related mitigation measures at nuclear facilities.

SAND2019-6135 A Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

Gender

State

United States

Primary authors: WILLIAMS, Adam (Sandia National Laboratories); Dr CHARLTON, William (Nuclear Engineering Teaching Laboratory, University of Texas); Mrs ABBOTT, Shannon (Sandia National Laboratories); Mrs CAMP, Noelle (Sandia National Laboratories); Mr WALLACE, Eric (Sandia National Laboratories); Mr ROSS, Michael (Sandia National Laboratories); Dr TERRY, James (Nuclear Engineering Teaching Laboratory, University of Texas)

Presenter: WILLIAMS, Adam (Sandia National Laboratories)

Track Classification: PP: Insider threats