Sandia National Laboratories

Evaluating the Effectiveness of Insider Threat Mitigation Systems

Sondra Spence, Gregory Baum, Steven Horowitz, Sandia National Laboratories
Joel Lewis, Thomas Edmunds, Lawrence Livermore National Laboratory
Tyler Cooperider, Claud R. Clark, Mary Lin Y-12 National Security Complex

June 2021

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

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-NA0003525.

ABSTRACT

Defending against the insider threat is a topic of increasing concern to the international nuclear community. Nuclear facilities must be able to evaluate the effectiveness of insider threat mitigation strategies and understand how to use results to strengthen and integrate those mitigations into a robust program. With support from the NNSA's Office of International Nuclear Security, subject matter experts (SMEs) have developed a series of workshops that provide the foundational knowledge needed to build and sustain an Insider Threat Evaluation Program. This paper and presentation define a systematic method for evaluating insider threat program effectiveness using documentation, assumption validation, and preventive and protective mitigation measurement to determine program quality and efficacy. The paper and presentation show how a hypothetical facility is used to deliver a series of customized workshops that apply a site-specific, graded approach to nuclear security, as recommended by the IAEA. The workshops also engage stakeholders with different responsibilities, roles, and engagement levels in the overall evaluation program, which serves to increase understanding and communication, and ultimately enables a more robust and sustainable program.

INTRODUCTION

Understanding how to evaluate the Insider Threat has been a long-standing challenge in the international community. Sparsity of data, and challenges collecting it, differing applications of mitigations across countries based on regulatory requirements and cultural norms, and many other factors have contributed to a lack of a standardized approached for evaluating the effectiveness of insider threat mitigations.

There is a robust body of international guidance describing types of mitigations and their potential modes of applications [1]. However, most of the effectiveness evaluation guidance is focused on the outsider threat.[2] With this challenge in mind, a series of workshops split into "tiers" was developed to enable the development of an insider effectiveness evaluation program, to describe the types of tools and methods that can be used in the evaluation process, and to a demonstrate application of the insider effectiveness evaluation process. This process is illustrated in **Figure 1**.

Figure 1Tier Outline for Workshop Series

This paper will outline each tier, the process behind its development, the content associated with each tier, and the desired learning outcomes for participants. It is important to note that the insider effectiveness evaluation is and should be a part of the larger system effectiveness evaluation program at the site as required by the regulatory requirements in country. It is not the intent of this paper or series of workshops to imply that the insider program should be separate. Additionally, the process, methods, and tools used in this workshop series were selected form a broad range of possibilities and are not the only approach that can be taken when evaluating effectiveness.

[1] IAEA NSS 8 Preventive and Protective Measures Against Insider Threats, IAEA EA TECDOC 967 Implementation of Physical Protection, IAEA NSS 27-G Physical Protection of Nuclear Material and Nuclear Facilities, and DOE Order O 470.5 Insider Threat Program.
[2] IAEA TECDOC 1868 Nuclear Assessment Methodologies for Regulated Facilities (2019), DOE-STD-1192 Security Risk Management Technical Standard, Volume II Vulnerability Assessments (2010).

TIER 1: BUILDING AN INSIDER EFFECTIVENESS EVALUATION PROGRAM

In order to build an effective program, it is vital that all parties involved across the states Nuclear Security Regime be fully involved and aware of their roles in supporting, creating, and maintaining the program. It is also important for all parties involved to understand, even at a high level, the process of evaluation and the methods being used at their facility. Without this understanding, no party involved can understand their impact on the program as a whole.

Tier one content is aimed at the stakeholders responsible for any part of the insider effectiveness evaluation program. It walks participants through the following elements.

- regulatory structures associated with the program
- necessary facility level programs, plans and procedures needed for an evaluation to be effective
- threats, targets, and characterizations of the facility that need to be in place
- the process of conducting the effectiveness evaluation and the methods and tools used to do so

This content is designed to foster communication and awareness across stakeholders.

The process of conducting a Vulnerability Assessment (VA) is a well-accepted systematic approach for gathering information to conduct evaluations against the outsider threat. For this reason, the structure of conducting a VA was used as the baseline for the conduct of the insider effectiveness evaluation, while noting the areas where the approach may be different than the traditional application to outsider threats. **Figure 2** is the outline followed for insider effectiveness evaluations.

Figure 2 Effectiveness Evaluation Process

The expected outcome of this tier is to provide the foundation to build effectiveness evaluation program components, to highlight implementation considerations, and to provide an effectiveness

evaluation program outline. Content for tier one is intended to be provided in a conference room/classroom setting over a period of 3-4 days. The content will be structured with presentations, exercises, and facilitated discussions with the partners focusing on primary topics associated with the development of an Insider Threat Mitigation effectiveness evaluation program. The tier one content will include an overview of the series and conclude with a high-level overview of tier two contents. This will give management present in tier one appropriate expectations about results of the continuing engagements and the appropriate audience for tiers two and three.

TIER 2: METHODS AND TOOLS USED IN AN EFFECTIVENESS EVALUATION PROGRAM

Tier two content facilitates a systematic method for evaluating system effectiveness against an insider threat and explains the various considerations needed on evaluation topics such as documentation, validating assumptions, and measuring preventive mitigations, and how all of those topics can directly impact the quality and effectiveness of the evaluation program. The goals of an effectiveness evaluation program are shown in **Figure 3**.

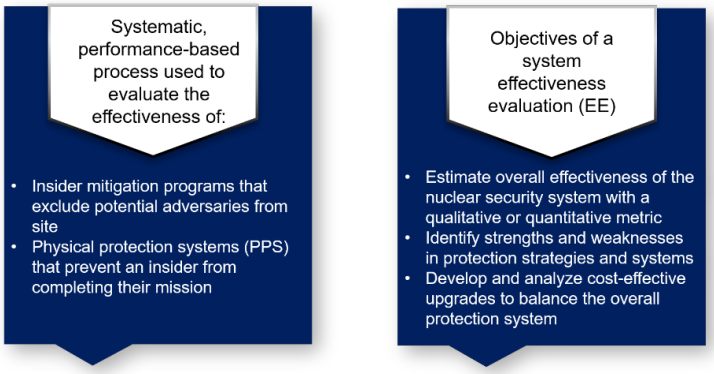

Figure 3 Goals of an Effectiveness Evaluation Program

One of the most important requirements of any effectiveness analysis is documentation and repeatability. Tier two provides participants with an outline of one process that could be used that is based on the VA outline discussed above. Throughout the entire tier, a hypothetical nuclear facility with all relevant documentation needed for the effectiveness evaluation process is used to illustrate the process. The handbook provides information needed to navigate through all of the presentations

and exercises. Part of Tier 2 focuses on conducting a vulnerability analysis specific to an insider threat. The content consists of:

- Planning and preparing for a Vulnerability Analysis
- Collecting and reviewing relevant data, including uncertainties and documentation of assumptions
- Analyzing system effectiveness using two analysis methods
- Determining the level of analysis needed to have confidence in the results
- Discussion of results, sensitivity analysis, and potential improvements in facility hardware or procedures
- Knowledge evaluation of participant progress throughout the tier

Part of the challenge in evaluating insider mitigations is how to validate the assumptions that are made about the level of effectiveness for individual mitigations. For example, there is a well-established process for determining an individual technological component's probability of detection (i.e. a passive infrared sensor can be performance tested to determine it alarms 80%[3] of the time). It is less clear how to develop such estimates for all preventive and protective mitigation measures against an insider. An additional challenge when looking at effectiveness evaluation is the potentially complex timeline of an insider attack. **Figure 4** below is a traditional adversary task timeline of an outsider attack. It outlines sensing, detection, assessment, and response components along that particular adversary pathway. It is assumed to be a continuous timeline of attack.

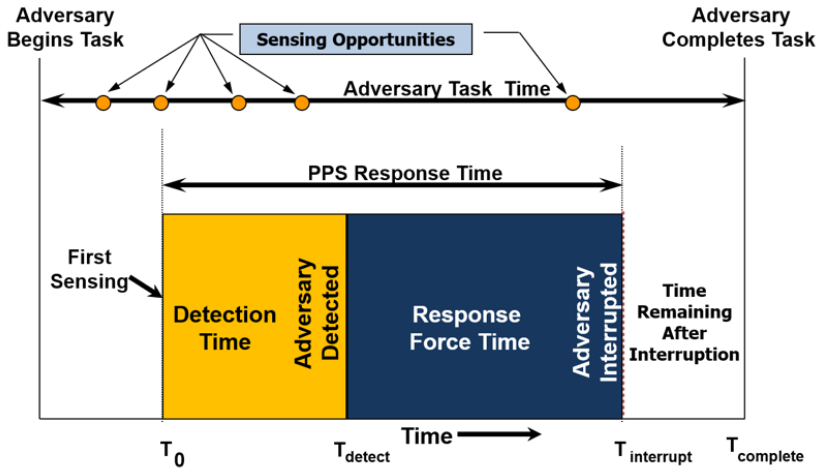

Figure 4 Outsider Adversary Task Timeline

[3] This is a hypothetical number used only for example purposes.

Because of insider's access, authority, and knowledge, one cannot necessarily assume that the timeline of attack will also be continuous. For example, an active insider may disable an alarm one day and execute the remaining steps in a threat scenario the next day exploiting the disabled alarm. The insider could also smuggle contraband into the facility for use at a later date. Outsider pathway analysis methods may not account for such complex, disjoint timelines. One of the main values of this workshop series is the opportunity for discussion and collaboration with subject matter experts to discuss these challenging problems, and how the global community can begin to address them.

Tier two content is primarily exercise and discussion driven, with subject matter experts leading practitioners through the content focusing on discussions regarding documentation of assumptions, applications of analysis tools and associated pros and cons, infrastructure and documentation needed to effectively evaluate programs, and where the insider evaluation fits into larger nuclear security system effectiveness evaluations.

Tier two uses two primary analysis methods in combination that complement the strengths and weaknesses of each. First, qualitative tabletop exercises are developed that allows for flexible scenario development and discussion about capabilities of an insider adversary based on their access, authority, and knowledge as well as policies and procedures at the facility. The second analysis tool is a simple quantitative method designed to give a rough estimate of system effectiveness against a scenario-based adversary pathway called the Security System Effectiveness Calculator (SSEC)[4].

The intended outcome of tier two is for participants to gain applied experience in the process, methods, and tools for evaluating insider threats using a hypothetical facility. Participants will be able to identify gaps in their current facility processes and programs, and what skills if any are needed to fill those gaps and create a robust effectiveness evaluation program that is indigenous and sustainable. Participants will leave with a needs analysis document that identifies topics covered in the course that they would like to focus on and have more in-depth technical discussions during tier three. Throughout tier two, instructors will utilize evaluations at to assess participant's comprehension. These simple evaluations will help instructors gauge an increase in participant

[4] Security System Effectiveness Calculator fact sheet, LLNL-BR-822434 (May 2021).

knowledge to ensure proper readiness for tier three activities. The tier two workshop is intended to be provided in a conference room / classroom setting over a period of 5-8 days.

TIER 3: DEMONSTRATED APPLICATION OF AN INSIDER EFFECTIVENESS EVALUATION PROGRAM

Tier three is essentially a repetition of the content of tier two, with one major difference. It is no longer instructor-led, but practitioner-driven. The process application will stay consistent, but the facility used, scenarios developed, and assumptions made can vary. Tier three is the most advanced step amongst the tiers working directly with participants to establish an effective and sustainable insider threat mitigation program for their own facility. Some level of customization for tier three will be required as it is heavily reliant on the partners existing capacity in various areas of the evaluation process.

As stated above, tier three will be more of a consultation role rather than the instructor-led environment in tier two. The transition allows the participants to become self-reliant moving through the effectiveness evaluation process. The exception to this step though may come when participants reach the requested areas for focus and improvement from tier two. This is where the SME instructors can transition back into the lead role to work through the requested areas with the participants to ensure the topics have been covered accurately and thoroughly. Depending on the areas of focus requested by the partners, tier three may be accomplished through one or several engagements over time until the partners have reached the level that an indigenous program now exists and can be sustained within their country. The intent in Tier 3 is to move participants from learning to application. Instructors will measure how well the participants apply their knowledge in as close to a real world setting as possible.

CONCLUSIONS

As this workshop series is intended to enable capacity building towards a sustained program, it is not expected that every participant will start or end at the same level of awareness. It is the intent to remain flexible and ensure follow-on discussions are continued. The makeup of those discussions could continue with the structure of tier three as more areas of focus are identified, or they could move into more of a technical exchange format depending on desired outcomes.

Evaluating the effectiveness of insider threat mitigation systems is a challenging and complex problem. Through this tiered approach, a systematic process for developing, implementing, and sustaining an insider threat program is expected to enhance awareness and communication with a variety of relevant stakeholders. While this is not the only possible approach, this series of workshops serves to deliver a robust and sustainable solution where guidance is incomplete. Furthermore, the framework of a flexible workshop series allows for a tailored approach sensitive to individual stakeholder facilities, needs, and cultures.