Information Design Assurance Red Team

IDART is a rigorous, time-proven assessment process that draws on deep cyber expertise from across the lab to perform adversary-based cybersecurity assessments.

IDART
Adversary-based Assessments

Introduction

Since 1996, Sandia National Laboratories (Sandia) has been using the IDART methodology to perform assessments on a broad range of complex networks, systems, and applications for government, military, and commercial industry. Our focus is risk-informed design assurance & vulnerability assessments for critical systems, non-traditional cyber-physical systems, and traditional cyber systems.

Methodology

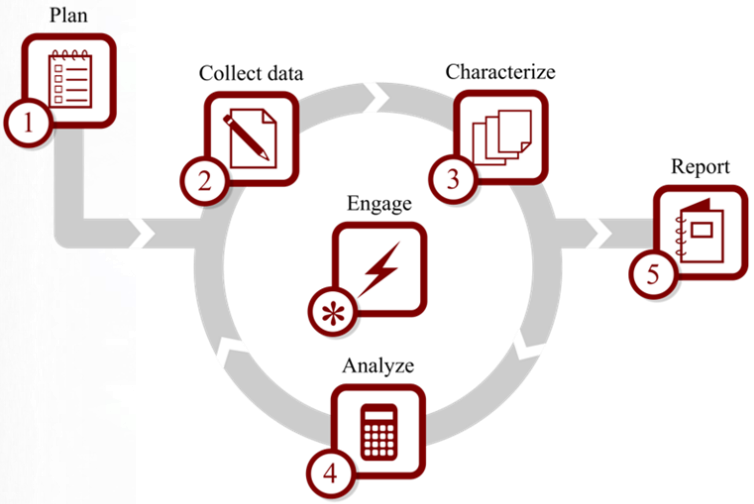
IDART is a NIST-recognized method in SP800-115, Technical Guide to Information Security Testing. The method has been improved over time to help sponsors better assess and understand risks presented by a spectrum of adversaries. It supports repeatable assessments with measurable results that can be used to make improvements and evaluate progress. Sandia's red teams perform IDART assessments to help stakeholders acquire an independent, objective view of system weaknesses using a range of adversary perspectives.

Besides assessment planning and reporting of results, core IDART assessment tasks include:

- Characterizing the target system and its architecture,
- Identifying nightmare consequences,
- Analyzing the system for its security strengths and weaknesses,
- Identifying potential vulnerabilities whose exploitation will result in nightmare consequences, and
- Providing prioritized mitigation strategies so owners can make risk-informed choices

IDART guides the red team to work closely with system developers, owners, and operators to allow for a more in-depth understanding of the system, to save time and resources, and to understand why the system is in its current state. This cooperative approach improves efficiency, enabling the red team to find as many attack paths as possible, and adds confidence in the analysis.

A range of adversary models is used to filter attack possibilities and assist in threat-based prioritization of protection strategies. These models include a spectrum of threats characterized by both measurable capabilities, such as knowledge, access, and resources, as well as, intangibles such as risk tolerance and motivation. Attacks are prioritized on difficulty and consequence.



Assessments at Sandia

Sandia's IDART red teaming approach is based on principles of systems engineering and includes a family of methods and tools. Assessments are strengthened by deep expertise in multi-disciplinary technical programs across the laboratories from domains including physical, cyber, nuclear, energy, and control systems security. Sandia's specialized assessment team can tailor the approach based on the complexity of the system, mission consequences, and adversary sophistication.

Assessment Experience and Improvement

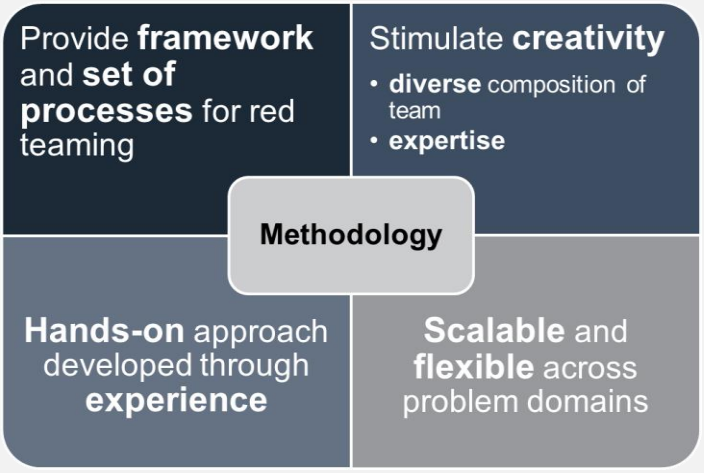
The IDART methodology has been utilized by Sandia to assess high-consequence systems for a range of sponsors including the U.S. government, military, industry, and critical infrastructure providers. To improve our accuracy, effectiveness, and completeness of results, we engage in research and development that advances assessment science and tools. We do this through both internally and externally funded research programs.

Experience, feedback, and lessons learned have been transformed into improvements and new analytic processes and methods. Sandia developed Red Teaming for Program Managers (RT4PM™) and Red Team Metrics to improve assessment planning and analysis, respectively. Adversary modeling has been substantially improved with the development of our Generic Threat Matrix.

When to Choose Sandia

Sandia National Laboratories is effective in providing a range of assessments adapted to complex and high-consequence systems, particularly when facing a range of capable adversaries or when existing within uncertain operating environments. IDART assessments can have the biggest impact when they are used to analyze systems and security technologies in design and development so that vulnerabilities can be addressed prior to deployment.

Sandia retains a wide range of security expertise in a variety of operational contexts; this subject matter expertise is integrated into IDART assessments to assist in the characterization and analysis of target systems. IDART is applicable to components, devices, networks, infrastructures, and world-wide enterprises.



Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

For more information:
idart@sandia.gov
http://www.idart.sandia.gov

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
SAND No. SAND2017-11967 M