

Information Operations Red Team & Assessments™ (IORTA™)

fact sheet

Independent, objective system assessments to improve design, identify vulnerabilities, threats, and make decisions about security options

Assessments and red teaming are often the tools of choice for decision makers in understanding their security risk, vulnerabilities, and defense posture. Yet problems exist in identifying specifics of these tools and the value they have in answering questions. What kind of assessment is needed? What is the quality? Is it actionable, measurable, and repeatable? Is the task bounded correctly to be efficient? Is it comprehensive and complete?

These and other questions are addressed in red teaming and assessments performed by the IORTA program. Sandia National Laboratories has developed and continues to refine assessments of systems, particularly those containing information flow and information technologies, in the IORTA program. Based upon a 50-year Sandia history of assessments, and strengthened by multi-disciplinary technical programs across Sandia, IORTA takes advantage of a wide variety of assessment and red teaming techniques, tools, and facilities to optimize results on a wide range of assessed systems throughout their lifecycle. Categories of IORTA assessments and red teaming activities include:

- Research & Development
- Operational Systems
- World-wide Enterprises
- Adversarial Modeling & Analysis
- C4I Architectures
- Security Architectures
- Development Exercises
- Critical Infrastructures, SCADA
- Security Devices, Cryptography
- Opposition Force Exercises
- Corporate Espionage
- Experiments & Demonstrations
- World Event Analysis
- Training, Tool Development

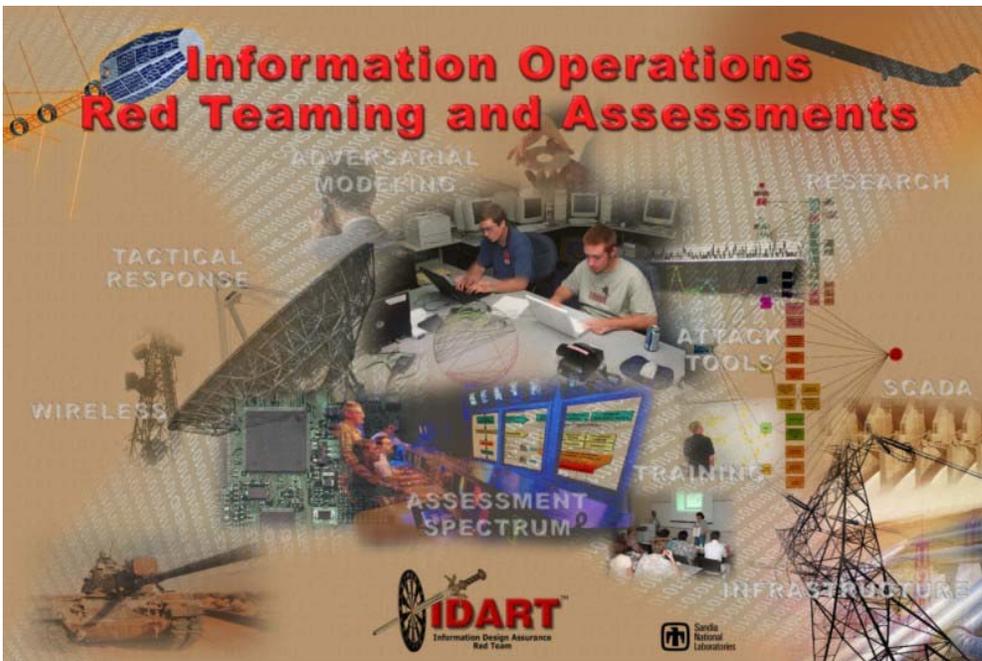
Multiple Methodologies

One approach, technique, or methodology is often insufficient to answer the needs of decision makers. IORTA considers a spectrum of assessment methodologies and tools to meet the needs of each assessment and optimize results. When planning an assessment, consideration is given to numerous variables including activity goals, maturity of system security, position in lifecycle, bounds and constraints of the assessment, as well as schedule and cost. The primary technique used is the IDART™ methodology, which is derived from IORTA's red team component – Information Design Assurance Red Team™; however, IORTA utilizes other methodologies from within and outside



of Sandia as required for a particular assessment. Even when the assessment does not call for red teaming, the IDART methodology and a malevolent adversarial view influence the process used to assess a system.

A key approach in IORTA is considering the security maturity of the system being assessed. If the system has no security policy or understanding of risk, it is unlikely that it will be able to withstand a sophisticated red team attack. In such a situation, a red team would easily penetrate the system. An eventual fix of the identified vulnerability would leave numerous others that the red team could exploit in the future. Therefore IORTA considers the maturity of a system's components and applies the appropriate methodology to each, such as risk assessment, IT management, IT security and red teaming. Additional methodologies include Opposition Force (OpFor) red teaming, which is used to exercise blue forces, develop adversary profiles, or generate adversary observables. The Tactical Red Team Analysis Cell (TRAC) provides hours-to-days response for urgent matters.



improvement of assessments and also externally for some agencies and groups. Training includes methodology and specific technical domains from a malevolent adversarial point of view.

Information Operations (IO)

In addition to cyber-induced effects on transmission of digital signals, IORTA considers system information effects including those induced by attack through means such as physical, electronic, human perception, social engineering, psychological operations, human factors, and system interdependencies.

Assessment Activities

The Right Team and Tools

In addition to multiple techniques, effective assessments require the right team and tools to obtain comprehensive answers about a system's vulnerabilities and security. A team is formed around a core group that understands IORTA assessment techniques and resources. They choose other members with appropriate expertise from around Sandia. These matrixed team members hone their skills in their own disciplines for their own customers, so provide leading-edge expertise for the assessment.

The resulting team is refined with appropriate tactical training on technique, technologies, and environmental knowledge. It is also enabled with other IORTA tools including specific methodologies, databases, libraries, attack resource labs, software toolsets, hardware systems, and project management staff. IORTA's techniques are refined through internal and external R&D. An important tool is adversarial modeling, which is required to generate measurable, consistent results in various IORTA's red teaming processes. A spectrum of outsiders and insiders is considered. IORTA's training program is a tool used both internally for

IORTA has assessed systems for U.S. and local government, military, industry, critical infrastructure providers, and foreign governments. Critical infrastructure systems IORTA has assessed include:

- Electric Generation & Transmission
- Banking & Finance
- Water (local & supply)
- Oil & Gas
- Telecommunications
- Transportation

IORTA engages in research and development to advance assessment science and tools through internal and externally funded research programs. Collaborations with government, industry, universities, and other government red teams are also pursued. Additional information is available on the IORTA web site given below.

For more information, contact:

Michael Skroch, Manager
 Information Operations Red Team & Assessments (IORTA)
 Sandia National Laboratories
 P.O. Box 5800; MS 0784
 Albuquerque, NM 87185-0784
 Phone: (505) 844-0104
 e-mail: mjskroc@sandia.gov

web: www.sandia.gov/iorta/
 web: www.sandia.gov/idart/



IDART is IORTA's Red Team



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company for the United States Department of Energy under Contract DE-AC04-94AL85000

v 030217

